Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)

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
Contents

Controlling the Multicast Flooding Time After a TCN Event 76
Recovering from Flood Mode 77
Disabling Multicast Flooding During a TCN Event 78
Configuring the IGMP Snooping Querier 80
Disabling IGMP Report Suppression 82
Configuring IGMP Profiles 83
Applying IGMP Profiles 85
Setting the Maximum Number of IGMP Groups 87
Configuring the IGMP Throttling Action 88
Monitoring IGMP Snooping 90
Monitoring IGMP Snooping Information 90
Monitoring IGMP Filtering 91
Configuration Examples for IGMP Snooping 92
   Example: Configuring IGMP Snooping Using CGMP Packets 92
   Example: Enabling a Static Connection to a Multicast Router 92
   Example: Configuring a Host Staticsly to Join a Group 92
   Example: Enabling IGMP Immediate Leave 92
   Example: Setting the IGMP Snooping Querier Source Address 92
   Example: Setting the IGMP Snooping Querier Maximum Response Time 93
   Example: Setting the IGMP Snooping Querier Timeout 93
   Example: Setting the IGMP Snooping Querier Feature 93
   Example: Configuring IGMP Profiles 93
   Example: Applying IGMP Profile 94
   Example: Setting the Maximum Number of IGMP Groups 94
Additional References 94
Feature History and Information for IGMP Snooping 95

CHAPTER 8

Configuring MLD Snooping 97
Finding Feature Information 97
Information About Configuring IPv6 MLD Snooping 97
Understanding MLD Snooping 97
   MLD Messages 98
   MLD Queries 98
   Multicast Client Aging Robustness 99
Multicast Router Discovery 99
MLD Reports 99
MLD Done Messages and Immediate-Leave 100
Topology Change Notification Processing 100
How to Configure IPv6 MLD Snooping 100
Default MLD Snooping Configuration 100
MLD Snooping Configuration Guidelines 101
Enabling or Disabling MLD Snooping on the Switch (CLI) 102
Enabling or Disabling MLD Snooping on a VLAN (CLI) 102
Configuring a Static Multicast Group 103
Configuring a Multicast Router Port (CLI) 104
Enabling MLD Immediate Leave (CLI) 105
Configuring MLD Snooping Queries (CLI) 106
Disabling MLD Listener Message Suppression (CLI) 107
Displaying MLD Snooping Information 108
Configuration Examples for Configuring MLD Snooping 109
Configuring a Static Multicast Group: Example 109
Configuring a Multicast Router Port: Example 109
Enabling MLD Immediate Leave: Example 109
Configuring MLD Snooping Queries: Example 109

PART III  IPv6  111

CHAPTER 9  Configuring IPv6 ACL  113
Finding Feature Information 113
Information About Configuring IPv6 ACLs 113
Understanding IPv6 ACLs 113
Supported ACL Features 114
IPv6 ACL Limitations 114
Configuring IPv6 ACLs 114
Default IPv6 ACL Configuration 115
Interaction with Other Features and Switches 115
Creating IPv6 ACL 115
Applying an IPv6 ACL to an Interface 119
PART IV  123

CHAPTER 10  125

Configuring Spanning Tree Protocol  125

Finding Feature Information  125
Restrictions for STP  125
Information About Spanning Tree Protocol  126

Spanning Tree Protocol  126

Spanning-Tree Topology and BPDUs  127
Bridge ID, Device Priority, and Extended System ID  128
Port Priority Versus Path Cost  129
Spanning-Tree Interface States  130
How a Switch or Port Becomes the Root Switch or Root Port  132
Spanning Tree and Redundant Connectivity  133
Spanning-Tree Address Management  134
Accelerated Aging to Retain Connectivity  134
Spanning-Tree Modes and Protocols  134
Supported Spanning-Tree Instances  135
Spanning-Tree Interoperability and Backward Compatibility  135
STP and IEEE 802.1Q Trunks  135
VLAN-Bridge Spanning Tree  136
Default Spanning-Tree Configuration  136
How to Configure Spanning-Tree Features  137

Changing the Spanning-Tree Mode (CLI)  137
Disabling Spanning Tree  138
Configuring the Root Switch  139
Configuring a Secondary Root Device  141
Configuring Port Priority  142
Configuring Path Cost  143
Configuring the Device Priority of a VLAN  145
CHAPTER 11  

Configuring Multiple Spanning-Tree Protocol  

Finding Feature Information  151  
Prerequisites for MSTP  151  
Restrictions for MSTP  152  
Information About MSTP  153  
MSTP Configuration  153  
MSTP Configuration Guidelines  153  
Root Switch  154  
Multiple Spanning-Tree Regions  154  
IST, CIST, and CST  155  
Operations Within an MST Region  156  
Operations Between MST Regions  156  
IEEE 802.1s Terminology  156  
Illustration of MST Regions  157  
Hop Count  158  
Boundary Ports  159  
IEEE 802.1s Implementation  159  
Port Role Naming Change  159  
Interoperation Between Legacy and Standard Switches  160  
Detecting Unidirectional Link Failure  160  
Interoperability with IEEE 802.1D STP  161  
RSTP Overview  161  
Port Roles and the Active Topology  161  
Rapid Convergence  162  
Synchronization of Port Roles  163  
Bridge Protocol Data Unit Format and Processing  164  
Topology Changes  165  
Protocol Migration Process  166
Default MSTP Configuration 166
About MST-to-PVST+ Interoperability (PVST+ Simulation) 167
About Detecting Unidirectional Link Failure 168
How to Configure MSTP Features 170
Specifying the MST Region Configuration and Enabling MSTP 170
Configuring the Root Switch 172
Configuring a Secondary Root Switch 173
Configuring Port Priority 174
Configuring Path Cost 176
Configuring the Switch Priority 177
Configuring the Hello Time 179
Configuring the Forwarding-Delay Time 180
Configuring the Maximum-Aging Time 181
Configuring the Maximum-Hop Count 182
Specifying the Link Type to Ensure Rapid Transitions 183
Designating the Neighbor Type 184
Restarting the Protocol Migration Process 185
Configuring PVST+ Simulation 186
Enabling PVST+ Simulation on a Port 187
Examples 188
Examples: PVST+ Simulation 188
Examples: Detecting Unidirectional Link Failure 192
Monitoring MST Configuration and Status 192
Feature Information for MSTP 193

CHAPTER 12

Configuring Optional Spanning-Tree Features 195
Finding Feature Information 195
Restriction for Optional Spanning-Tree Features 195
Information About Optional Spanning-Tree Features 196
PortFast 196
BPDU Guard 196
BPDU Filtering 197
UplinkFast 197
BackboneFast 199
EtherChannel Guard 201
Root Guard 202
Loop Guard 203
STP PortFast Port Types 203
Bridge Assurance 204

How to Configure Optional Spanning-Tree Features 206
   Enabling PortFast 206
   Enabling BPDU Guard 208
   Enabling BPDU Filtering 209
   Enabling UplinkFast for Use with Redundant Links 210
   Disabling UplinkFast 212
   Enabling BackboneFast 213
   Enabling EtherChannel Guard 214
   Enabling Root Guard 215
   Enabling Loop Guard 216
   Enabling PortFast Port Types 217
      Configuring the Default Port State Globally 218
      Configuring PortFast Edge on a Specified Interface 219
      Configuring a PortFast Network Port on a Specified Interface 220
   Enabling Bridge Assurance 221
Examples 222
   Examples: Configuring PortFast Edge on a Specified Interface 222
   Examples: Configuring a PortFast Network Port on a Specified Interface 223
   Example: Configuring Bridge Assurance 224
Monitoring the Spanning-Tree Status 225
Feature Information for Optional Spanning-Tree Features 225

CHAPTER 13

Configuring EtherChannels 227
   Finding Feature Information 227
   Restrictions for EtherChannels 227
   Information About EtherChannels 228
   EtherChannel Overview 228
      EtherChannel Modes 228
      EtherChannel on Switches 229
Contents

EtherChannel Link Failover 230
Channel Groups and Port-Channel Interfaces 230
Port Aggregation Protocol 231
  PAgP Modes 232
  PAgP Learn Method and Priority 233
  PAgP Interaction with Virtual Switches and Dual-Active Detection 234
  PAgP Interaction with Other Features 234
Link Aggregation Control Protocol 234
  LACP Modes 235
  LACP Interaction with Other Features 235
EtherChannel On Mode 235
EtherChannel Load Deferral Overview 236
Default EtherChannel Configuration 237
EtherChannel Configuration Guidelines 238
  Layer 2 EtherChannel Configuration Guidelines 239
Auto-LAG 239
  Auto-LAG Configuration Guidelines 240
How to Configure EtherChannels 241
  Configuring Layer 2 EtherChannels 241
  Configuring Port Channel Load Deferral 243
  Configuring the PAgP Learn Method and Priority 245
  Configuring LACP Hot-Standby Ports 247
    Configuring the LACP System Priority 247
    Configuring the LACP Port Priority 248
  Configuring the LACP Port Channel Min-Links Feature 250
  Configuring LACP Fast Rate Timer 251
  Configuring Auto-LAG Globally 252
  Configuring Auto-LAG on a Port Interface 253
  Configuring Persistence with Auto-LAG 254
Monitoring EtherChannel, PAgP, and LACP Status 255
Configuration Examples for Configuring EtherChannels 256
  Configuring Layer 2 EtherChannels: Examples 256
  Example: Configuring Port Channel Load Deferral 257
  Configuring Auto LAG: Examples 257
CHAPTER 14

Configuring the MAC Address-Table Move Update Feature 261
Finding Feature Information 261
Information About MAC Address-Table Move Update 261
MAC Address-Table Move Update 261
MAC Address-Table Move Update Configuration Guidelines 263
How to Configure MAC Address-Table Move Update 263
Configuring MAC Address-Table Move Update 263
Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages 264
Monitoring the MAC Address-Table Move Update 265
Configuration Examples for MAC Address-Table Move Update 265
Configuring the MAC Address-Table Move Update: Examples 265

CHAPTER 15

Configuring UniDirectional Link Detection 267
Finding Feature Information 267
Restrictions for Configuring UDLD 267
Information About UDLD 268
Modes of Operation 268
Normal Mode 268
Aggressive Mode 268
Methods to Detect Unidirectional Links 269
Neighbor Database Maintenance 269
Event-Driven Detection and Echoing 269
UDLD Reset Options 270
Default UDLD Configuration 270
How to Configure UDLD 270
Enabling UDLD Globally 270
Enabling UDLD on an Interface 272
Monitoring and Maintaining UDLD 273
Additional References for UDLD 273
CHAPTER 18

Configuring Simple Network Management Protocol  301
Finding Feature Information  301
Prerequisites for SNMP  301
Restrictions for SNMP  303
Information About SNMP  304
   SNMP Overview  304
   SNMP Manager Functions  304
   SNMP Agent Functions  304
   SNMP Community Strings  305
   SNMP MIB Variables Access  305
   SNMP Notifications  306
   SNMP ifIndex MIB Object Values  306
Default SNMP Configuration  307
SNMP Configuration Guidelines  307
How to Configure SNMP  308
   Disabling the SNMP Agent  308
   Configuring Community Strings  309
   Configuring SNMP Groups and Users  312
   Configuring SNMP Notifications  315
   Setting the Agent Contact and Location Information  319
   Limiting TFTP Servers Used Through SNMP  321
Monitoring SNMP Status  322
SNMP Examples  323
Additional References  324
Feature History and Information for Simple Network Management Protocol  325

CHAPTER 19

Configuring SPAN  327
Finding Feature Information  327
QoS 413

CHAPTER 26 Configuring QoS 415

Finding Feature Information 415
Prerequisites for QoS 415
  General QoS Guidelines 415
Restrictions for QoS 416
Information About QoS 416
QoS Implementation 416
  Layer 2 Frame Prioritization Bits 417
  Layer 3 Packet Prioritization Bits 417
QoS Basic Model 418
  Actions at Ingress Port 418
  Actions at Egress Port 418
Mapping Tables Overview 419
Queueing and Scheduling Overview 420
Queueing and Scheduling on Egress Queues 420
Packet Modification 424
Standard QoS Default Configuration 424
  Default Egress Queue Configuration 424
  Default Mapping Table Configuration 425
How to Configure QoS 425
  Enabling QoS Globally 425
  Enabling VLAN-Based QoS on Physical Ports 426
Configuring a QoS Policy 428
  Classifying Traffic by Using ACLs 428
  Classifying Traffic by Using Class Maps 436
  Classifying Traffic by Using Class Maps and Filtering IPv6 Traffic 438
  Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps 440
Classifying, Policing, and Marking Traffic by Using Aggregate Policers 445
Configuring Egress Queue Characteristics 447
  Configuration Guidelines 448
  Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set 448
  Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID 449
  Configuring SRR Shaped Weights on Egress Queues 452
  Configuring SRR Shared Weights on Egress Queues 454
  Configuring the Egress Expedite Queue 455
  Limiting the Bandwidth on an Egress Interface 457
Monitoring Standard QoS 458
Configuration Examples for QoS 459
  Example: Configuring Port to the DSCP-Trusted State and Modifying the DSCP-to-DSCP-Mutation Map 459
  Examples: Classifying Traffic by Using ACLs 459
  Examples: Classifying Traffic by Using Class Maps 460
  Examples: Classifying, Policing, and Marking Traffic on Physical Ports Using Policy Maps 462
  Examples: Classifying, Policing, and Marking Traffic by Using Aggregate Policers 463
  Examples: Configuring DSCP Maps 464
  Examples: Configuring Egress Queue Characteristics 466
Where to Go Next 467

PART IX  Security 469

CHAPTER 27  Security Features Overview 471
  Security Features Overview 471

CHAPTER 28  Preventing Unauthorized Access 475
  Finding Feature Information 475
  Preventing Unauthorized Access 475

CHAPTER 29  Controlling Switch Access with Passwords and Privilege Levels 477
  Finding Feature Information 477
  Restrictions for Controlling Switch Access with Passwords and Privileges 477
  Information About Passwords and Privilege Levels 478
Default Password and Privilege Level Configuration 478
Additional Password Security 478
Password Recovery 478
Terminal Line Telnet Configuration 479
Username and Password Pairs 479
Privilege Levels 479

How to Control Switch Access with Passwords and Privilege Levels 480
Setting or Changing a Static Enable Password 480
Protecting Enable and Enable Secret Passwords with Encryption 482
Disabling Password Recovery 483
Setting a Telnet Password for a Terminal Line 485
Configuring Username and Password Pairs 486
Setting the Privilege Level for a Command 488
Changing the Default Privilege Level for Lines 490
Logging into and Exiting a Privilege Level 491

Monitoring Switch Access 492
Configuration Examples for Setting Passwords and Privilege Levels 492
  Example: Setting or Changing a Static Enable Password 492
  Example: Protecting Enable and Enable Secret Passwords with Encryption 492
  Example: Setting a Telnet Password for a Terminal Line 492
  Example: Setting the Privilege Level for a Command 493

Additional References 493

CHAPTER 30

Configuring TACACS+ 495
Finding Feature Information 495
Prerequisites for TACACS+ 495
Restrictions for TACACS+ 496
Information About TACACS+ 497
  TACACS+ and Switch Access 497
  TACACS+ Overview 497
  TACACS+ Operation 498
Method List 499
TACACS AV Pairs 499
  TACACS Authentication and Authorization AV Pairs 499
CHAPTER 32

Configuring Accounting  581

Finding Feature Information  581
Prerequisites for Configuring Accounting  581
Restrictions for Configuring Accounting  582
Information About Configuring Accounting  582

Named Method Lists for Accounting  582
  Method Lists and Server Groups  583
  AAA Accounting Methods  583
  Accounting Record Types  584
  AAA Accounting Methods  584

AAA Accounting Types  584
  Network Accounting  584
  EXEC Accounting  587
  Command Accounting  588
  Connection Accounting  589
  System Accounting  591
  Resource Accounting  591
  VRSS Accounting  593

AAA Accounting Enhancements  594
  AAA Broadcast Accounting  594
  AAA Session MIB  594
  Accounting Attribute-Value Pairs  595

How to Configure Accounting  595
  Configuring AAA Accounting Using Named Method Lists  595
  Configuring RADIUS System Accounting  597
  Suppressing Generation of Accounting Records for Null Username Sessions  598
  Generating Interim Accounting Records  598
  Generating Accounting Records for Failed Login or Session  599
  Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records  599
  Configuring AAA Resource Failure Stop Accounting  600
  Configuring AAA Resource Accounting for Start-Stop Records  600
  Configuring AAA Broadcast Accounting  600
CHAPTER 33

Configuring Local Authentication and Authorization 611
Finding Feature Information 611
How to Configure Local Authentication and Authorization 611
  Configuring the Switch for Local Authentication and Authorization 611
Monitoring Local Authentication and Authorization 613
Additional References 614
Feature Information for Local Authentication and Authorization 614

CHAPTER 34

MAC Authentication Bypass 615
Finding Feature Information 615
Prerequisites for Configuring MAC Authentication Bypass 615
Information About MAC Authentication Bypass 616
  Overview of the Cisco IOS Auth Manager 616
  Overview of the Configurable MAB Username and Password 616
How to Configure MAC Authentication Bypass 617
  Enabling MAC Authentication Bypass 617
  Enabling Reauthentication on a Port 619
  Specifying the Security Violation Mode 620
Password Strength and Management for Common Criteria 627
Finding Feature Information 627
Restrictions for Password Strength and Management for Common Criteria 628
Information About Password Strength and Management for Common Criteria 628
  Password Composition Policy 628
  Password Length Policy 628
  Password Lifetime Policy 628
  Password Expiry Policy 628
  Password Change Policy 629
  User Reauthentication Policy 629
  Support for Framed (noninteractive) Session 629
How to Configure Password Strength and Management for Common Criteria 630
  Configuring the Password Security Policy 630
  Verifying the Common Criteria Policy 632
Configuration Examples for Password Strength and Management for Common Criteria 633
  Example: Password Strength and Management for Common Criteria 633
Additional References for Password Strength and Management for Common Criteria 633
Feature Information for Password Strength and Management for Common Criteria 634

AAA-SERVER-MIB Set Operation 637
Finding Feature Information 637
Prerequisites for AAA-SERVER-MIB Set Operation 637
Restrictions for AAA-SERVER-MIB Set Operation 638
Information About AAA-SERVER-MIB Set Operation 638
  CISCO-AAA-SERVER-MIB 638
  CISCO-AAA-SERVER-MIB Set Operation 638
How to Configure AAA-SERVER-MIB Set Operation 638
CHAPTER 37 Configuring Secure Shell 645
Finding Feature Information 645
Prerequisites for Configuring Secure Shell 645
Restrictions for Configuring Secure Shell 646
Information about SSH 646
  SSH and Switch Access 646
  SSH Servers, Integrated Clients, and Supported Versions 647
  RSA Authentication Support 647
  SSL Configuration Guidelines 647
  Secure Copy Protocol Overview 647
  Secure Copy Protocol 648
  How Secure Copy Works 648
  Reverse Telnet 648
  Reverse SSH 649
How to Configure Secure Shell 649
  Setting Up the Switch to Run SSH 649
  Configuring the SSH Server 650
  Invoking an SSH Client 652
  Troubleshooting Tips 653
  Configuring Reverse SSH for Console Access 653
  Configuring Reverse SSH for Modem Access 655
  Troubleshooting Reverse SSH on the Client 657
  Troubleshooting Reverse SSH on the Server 657
  Monitoring the SSH Configuration and Status 658
  Configuring Secure Copy 658
Configuration Examples for Secure Shell 660
  Example: Secure Copy Configuration Using Local Authentication 660
Chapter 41 Certification Authority Interoperability

Finding Feature Information 717
Prerequisites For Certification Authority 717
Restrictions for Certification Authority 717
Information About Certification Authority 718
CA Supported Standards 718
Purpose of CAs 718
Implementing IPsec Without CAs 719
Implementing IPsec With CAs 719
Implementing IPsec with Multiple Root CAs 720
How CA Certificates Are Used by IPsec Devices 720
Registration Authorities 721
How to Configure Certification Authority 721
Managing NVRAM Memory Usage 721
Configuring the Device Host Name and IP Domain Name 722
Generating an RSA Key Pair 723
Declaring a Certification Authority 723
Configuring a Root CA (Trusted Root) 725
Authenticating the CA 726
Requesting Signed Certificates 727
Monitoring and Maintaining Certification Authority 728
Requesting a Certificate Revocation List 728
Querying a Certificate Revocation List 729
Deleting RSA Keys from a Device 730
Deleting Public Keys for a Peer 731
Contents

Deleting Certificates from the Configuration 732
Viewing Keys and Certificates 733

CHAPTER 42

Access Control List Overview 735
Finding Feature Information 735
Information About Access Control Lists 735
Definition of an Access List 735
Functions of an Access Control List 736
Purpose of IP Access Lists 736
Reasons to Configure ACLs 737
Software Processing of an Access List 737
Access List Rules 738
Helpful Hints for Creating IP Access Lists 738
IP Packet Fields You Can Filter to Control Access 739
Source and Destination Addresses 739
Wildcard Mask for Addresses in an Access List 740
Access List Sequence Numbers 740
ACL Supported Types 741
Supported ACLs 741
Port ACLs 741
Access Control Entries 742
ACEs and Fragmented and Unfragmented Traffic 742
ACEs and Fragmented and Unfragmented Traffic Examples 742

CHAPTER 43

Configuring IPv4 Access Control Lists 745
Finding Feature Information 745
Restrictions for Configuring IPv4 Access Control Lists 745
Information About Configuring IPv4 Access Control Lists 746
ACL Overview 746
Standard and Extended IPv4 ACLs 747
IPv4 ACL Switch Unsupported Features 747
Access List Numbers 747
Numbered Standard IPv4 ACLs 748
Numbered Extended IPv4 ACLs 749
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Named IPv4 ACLs</td>
<td>749</td>
</tr>
<tr>
<td>Benefits of IP Access List Entry Sequence Numbering</td>
<td>750</td>
</tr>
<tr>
<td>Sequence Numbering Behavior</td>
<td>750</td>
</tr>
<tr>
<td>Including comments in ACLs</td>
<td>751</td>
</tr>
<tr>
<td>Hardware and Software Treatment of IP ACLs</td>
<td>751</td>
</tr>
<tr>
<td>Time Ranges for ACLs</td>
<td>752</td>
</tr>
<tr>
<td>IPv4 ACL Interface Considerations</td>
<td>752</td>
</tr>
<tr>
<td>Apply an Access Control List to an Interface</td>
<td>753</td>
</tr>
<tr>
<td>ACL Logging</td>
<td>754</td>
</tr>
<tr>
<td>How to Configure ACLs</td>
<td>754</td>
</tr>
<tr>
<td>Configuring IPv4 ACLs</td>
<td>754</td>
</tr>
<tr>
<td>Creating a Numbered Standard ACL</td>
<td>755</td>
</tr>
<tr>
<td>Creating a Numbered Extended ACL</td>
<td>756</td>
</tr>
<tr>
<td>Creating Named Standard ACL</td>
<td>759</td>
</tr>
<tr>
<td>Creating Extended Named ACL</td>
<td>761</td>
</tr>
<tr>
<td>Sequencing Access-List Entries and Revising the Access List</td>
<td>763</td>
</tr>
<tr>
<td>Configuring Commented IP ACL Entries</td>
<td>766</td>
</tr>
<tr>
<td>Configuring Time Ranges for ACLs</td>
<td>767</td>
</tr>
<tr>
<td>Applying an IPv4 ACL to a Terminal Line</td>
<td>768</td>
</tr>
<tr>
<td>Applying an IPv4 ACL to an Interface</td>
<td>770</td>
</tr>
<tr>
<td>Monitoring IPv4 ACLs</td>
<td>771</td>
</tr>
<tr>
<td>Configuration Examples for ACLs</td>
<td>772</td>
</tr>
<tr>
<td>ACLs in a Small Networked Office</td>
<td>772</td>
</tr>
<tr>
<td>Example: Numbered ACLs</td>
<td>772</td>
</tr>
<tr>
<td>Examples: Extended ACLs</td>
<td>773</td>
</tr>
<tr>
<td>Examples: Named ACLs</td>
<td>774</td>
</tr>
<tr>
<td>Example Resequencing Entries in an Access List</td>
<td>774</td>
</tr>
<tr>
<td>Example Adding an Entry with a Sequence Number</td>
<td>775</td>
</tr>
<tr>
<td>Example Adding an Entry with No Sequence Number</td>
<td>775</td>
</tr>
<tr>
<td>Examples: Configuring Commented IP ACL Entries</td>
<td>776</td>
</tr>
<tr>
<td>Examples: Using Time Ranges with ACLs</td>
<td>776</td>
</tr>
<tr>
<td>Examples: Time Range Applied to an IP ACL</td>
<td>777</td>
</tr>
<tr>
<td>Examples: ACL Logging</td>
<td>777</td>
</tr>
<tr>
<td>Examples: Troubleshooting ACLs</td>
<td>779</td>
</tr>
</tbody>
</table>
CHAPTER 44 IPv6 Access Control Lists 783
Finding Feature Information 783
Restrictions for IPv6 ACLs 783
Information About Configuring IPv6 ACLs 784
ACL Overview 784
IPv6 ACLs Overview 785
Interactions with Other Features and Switches 785
Default Configuration for IPv6 ACLs 785
Supported ACL Features 785
IPv6 Port-Based Access Control List Support 786
ACLs and Traffic Forwarding 786
How to Configure IPv6 ACLs 786
Configuring IPv6 ACLs 786
Attaching an IPv6 ACL to an Interface 790
Monitoring IPv6 ACLs 791
Configuring PACL Mode and Applying IPv6 PACL on an Interface 792
Configuring IPv6 ACL Extensions for Hop by Hop Filtering 793
Configuration Examples for IPv6 ACLs 794
Example: Configuring IPv6 ACLs 794
Example: Configuring PACL Mode and Applying IPv6 PACL on an Interface 795
Example: IPv6 ACL Extensions for Hop by Hop Filtering 795
Additional References 796
Feature Information for IPv6 Access Control Lists 796

CHAPTER 45 Configuring DHCP 799
Finding Feature Information 799
Information About DHCP 799
DHCP Server 799
DHCP Relay Agent 799
DHCP Snooping 800
Option-82 Data Insertion 801
Cisco IOS DHCP Server Database 804
DHCP Snooping Binding Database 804
How to Configure DHCP Features 806
Default DHCP Snooping Configuration 806
DHCP Snooping Configuration Guidelines 807
Configuring the DHCP Server 807
Configuring the DHCP Relay Agent 807
Specifying the Packet Forwarding Address 808
Prerequisites for Configuring DHCP Snooping and Option 82 810
Enabling DHCP Snooping and Option 82 811
Enabling the Cisco IOS DHCP Server Database 815
Monitoring DHCP Snooping Information 815
Configuring DHCP Server Port-Based Address Allocation 815
Information About Configuring DHCP Server Port-Based Address Allocation 815
Default Port-Based Address Allocation Configuration 816
Port-Based Address Allocation Configuration Guidelines 816
Enabling the DHCP Snooping Binding Database Agent 816
Enabling DHCP Server Port-Based Address Allocation 818
Monitoring DHCP Server Port-Based Address Allocation 820
Additional References 820
Feature Information for DHCP Snooping and Option 82 821

CHAPTER 46
Configuring IEEE 802.1x Port-Based Authentication 823
Finding Feature Information 823
How to Configure 802.1x Port-Based Authentication 823
Default 802.1x Authentication Configuration 823
802.1x Authentication Configuration Guidelines 825

802.1x Authentication 825
VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass 826
MAC Authentication Bypass 827
Maximum Number of Allowed Devices Per Port 827
Configuring 802.1x Violation Modes 827
Configuring 802.1x Authentication 829
Contents

Information About Performing Switch Setup Configuration 935
  Boot Process 935
  Switches Information Assignment 936
  Default Switch Information 936
  DHCP-Based Autoconfiguration Overview 937
    DHCP Client Request Process 937
  DHCP-based Autoconfiguration and Image Update 938
    Restrictions for DHCP-based Autoconfiguration 938
  DHCP Autoconfiguration 939
  DHCP Auto-Image Update 939
  DHCP Server Configuration Guidelines 939
    Purpose of the TFTP Server 940
    Purpose of the DNS Server 941
  Configuring Deep Sleep 941
  How to Obtain Configuration Files 941
  How to Control Environment Variables 942
    Common Environment Variables 943
    Environment Variables for TFTP 944
  Scheduled Reload of the Software Image 944
How to Perform Switch Setup Configuration 945
  Using the Smartphone App 945
  Configuring DHCP Autoconfiguration (Only Configuration File) 946
  Configuring DHCP Auto-Image Update (Configuration File and Image) 948
  Configuring the Client to Download Files from DHCP Server 951
  Routing Assistance When IP Routing is Disabled 952
    Default Gateway 952
  Configuring the NVRAM Buffer Size 953
  Configuring the Switch to Enter Deep Sleep Mode 954
  Configuring the Switch to Wake Up From Deep Sleep Mode 955
  Modifying the Switch Startup Configuration 956
    Specifying the Filename to Read and Write the System Configuration 956
    Manually Booting the Switch 957
    Configuring a Scheduled Software Image Reload 958
  Monitoring Switch Setup Configuration 959
### Example: Verifying the Switch Running Configuration

#### 959

- Examples: Displaying Software Install
- Configuration Examples for Performing Switch Setup
- Example: Configuring a Switch as a DHCP Server
- Example: Configuring DHCP Auto-Image Update
- Example: Configuring a Switch to Download Configurations from a DHCP Server
- Example: Configuring NVRAM Buffer Size

### Additional References for Performing Switch Setup

- Feature History and Information For Performing Switch Setup Configuration

---

### CHAPTER 50

#### Configuring System Message Logs

- Restrictions for Configuring System Message Logs
- Information About Configuring System Message Logs
  - System Message Logging
  - System Log Message Format
  - Default System Message Logging Settings
  - Enabling Syslog Trap Messages
- How to Configure System Message Logs
  - Setting the Message Display Destination Device
  - Synchronizing Log Messages
  - Disabling Message Logging
  - Enabling and Disabling Time Stamps on Log Messages
  - Enabling and Disabling Sequence Numbers in Log Messages
  - Defining the Message Severity Level
  - Limiting Syslog Messages Sent to the History Table and to SNMP
  - Logging Messages to a UNIX Syslog Daemon
- Monitoring and Maintaining System Message Logs
  - Monitoring Configuration Archive Logs
- Configuration Examples for System Message Logs
  - Example: Switch System Message
  - Examples: Displaying Service Timestamps Log
- Additional References for System Message Logs
- Feature History and Information For System Message Logs
PART XII

CHAPTER 54

Configuring VTP 1065
Finding Feature Information 1065
Prerequisites for VTP 1065
Restrictions for VTP 1066
Information About VTP 1066
VTP 1066
VTP Domain 1066
VTP Modes 1067
VTP Advertisements 1068
VTP Version 2 1069
Default Layer 2 Ethernet Interface VLAN Configuration 1109

How to Configure VLAN Trunks 1109
Configuring an Ethernet Interface as a Trunk Port 1109
Configuring a Trunk Port 1109
 Defining the Allowed VLANs on a Trunk 1111
Changing the Pruning-Eligible List 1113
Configuring the Native VLAN for Untagged Traffic 1114
Configuring Trunk Ports for Load Sharing 1116
Configuring Load Sharing Using STP Port Priorities 1116
Configuring Load Sharing Using STP Path Cost 1120

Configuration Examples for VLAN Trunking 1122
Example: Configuring a Trunk Port 1122
Example: Removing a VLAN from a Port 1123

Where to Go Next 1123
Additional References 1123
Feature History and Information for VLAN Trunks 1124

CHAPTER 57
Configuring VMPS 1125
Finding Feature Information 1125
Prerequisites for VMPS 1125
Restrictions for VMPS 1126
Information About VMPS 1126
 Dynamic VLAN Assignments 1126
 Dynamic-Access Port VLAN Membership 1127
Default VMPS Client Configuration 1128

How to Configure VMPS 1128
Entering the IP Address of the VMPS 1128
Configuring Dynamic-Access Ports on VMPS Clients 1129
Reconfirming VLAN Memberships 1131
Changing the Reconfirmation Interval 1132
Changing the Retry Count 1133
Troubleshooting Dynamic-Access Port VLAN Membership 1134
Monitoring the VMPS 1135
Configuration Example for VMPS 1135
Preface

This book describes configuration information and examples for the switch.

- Document Conventions, on page li
- Related Documentation, on page liii
- Obtaining Documentation and Submitting a Service Request, on page liii

Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in bold font.</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in courier font.</td>
</tr>
<tr>
<td><strong>Bold Courier</strong> font</td>
<td><strong>Bold Courier</strong> font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;:</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**Reader Alert Conventions**

This document may use the following conventions for reader alerts:

- **Note**
  - Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

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

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

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

- **Warning**
  - **IMPORTANT SAFETY INSTRUCTIONS**
    - This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

    **SAVE THESE INSTRUCTIONS**
Related Documentation

Note

Before installing or upgrading the switch, refer to the switch release notes.

- Cisco Validated Designs documents, located at:
  
  http://www.cisco.com/go/designzone

Obtaining Documentation and Submitting a Service Request

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


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

Interface and Hardware

• Configuring Interface Characteristics, on page 1
• Configuring Auto-MDIX, on page 27
• Configuring LLDP, LLDP-MED, and Wired Location Service, on page 31
• Configuring System MTU, on page 45
• Configuring PoE, on page 49
• Configuring EEE, on page 51
CHAPTER 1

Configuring Interface Characteristics

• Finding Feature Information, on page 1
• Information About Configuring Interface Characteristics, on page 1
• How to Configure Interface Characteristics, on page 9
• Monitoring Interface Characteristics, on page 20
• Configuration Examples for Interface Characteristics, on page 22
• Additional References for the Interface Characteristics Feature, on page 24
• Feature History and Information for Configuring Interface Characteristics, on page 25

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring Interface Characteristics

Interface Types

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

Note

The stack ports on the rear of the stacking-capable switches 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 switch 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 switch are assigned to a
VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch; the switch 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 switch 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 switch. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch 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 switch 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.

**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 switches or between switches 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 switch 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 switch has three USB ports on the front panel — a USB mini-Type B console port and two USB Type A ports.

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

**USB Mini-Type B Console Port**

The switch 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 switch. The connected device must include a terminal emulation application. When the switch 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 switch shows which console connection is in use.

**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 switch, to the router, back to the switch, and then to Host B.

*Figure 1: Connecting VLANs with the Switch*

![Diagram of connecting VLANs with the switch](image)

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

**Interface Configuration Mode**

The switch supports these interface types:

- Physical ports—switch 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 switch 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, gigabitethernet0/1 or gigabitethernet0/8. 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 switch, enter this command:

  ```
  Switch(config)# interface gigabitethernet0/4
  ```

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

  ```
  Switch(config)# interface gigabitethernet0/4
  ```

## Default Ethernet Interface Configuration

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

### Table 1: Default Layer 2 Ethernet Interface Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating mode</td>
<td>Layer 2 or switching mode (<strong>switchport</strong> command).</td>
</tr>
<tr>
<td>Allowed VLAN range</td>
<td>VLANs 1–4094.</td>
</tr>
<tr>
<td>Default VLAN (for access ports)</td>
<td>VLAN 1.</td>
</tr>
<tr>
<td>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Native VLAN (for IEEE 802.1Q trunks)</td>
<td>VLAN 1.</td>
</tr>
<tr>
<td>802.1p priority-tagged traffic</td>
<td>Drop all packets tagged with VLAN 0.</td>
</tr>
<tr>
<td>VLAN trunking</td>
<td>Switchport mode dynamic auto (supports DTP).</td>
</tr>
<tr>
<td>Port enable state</td>
<td>All ports are enabled.</td>
</tr>
<tr>
<td>Port description</td>
<td>None defined.</td>
</tr>
<tr>
<td>Speed</td>
<td>Autonegotiate. (Not supported on the 10-Gigabit interfaces.)</td>
</tr>
<tr>
<td>Duplex mode</td>
<td>Autonegotiate. (Not supported on the 10-Gigabit interfaces.)</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control is set to <strong>receive: off</strong>. It is always off for sent packets.</td>
</tr>
<tr>
<td>EtherChannel (PAgP)</td>
<td>Disabled on all Ethernet ports.</td>
</tr>
<tr>
<td>Port blocking (unknown multicast and unknown unicast traffic)</td>
<td>Disabled (not blocked).</td>
</tr>
<tr>
<td>Broadcast, multicast, and unicast storm control</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Protected port</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Port security</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Port Fast</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Auto-MDIX</td>
<td>Enabled.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The switch 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 switch through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port.</td>
</tr>
<tr>
<td>Power over Ethernet (PoE)</td>
<td>Enabled (auto).</td>
</tr>
<tr>
<td>Keepalive messages</td>
<td>Disabled on SFP module ports; enabled on all other ports.</td>
</tr>
</tbody>
</table>

### 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 models 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 `nongotiate` 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.

  **Note**
  * Catalyst 2960-L Switches do not support GLC-T and GLC-TE at speed 10/100 Mb/s.

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

You use the `flowcontrol` interface configuration command to set the interface’s ability to receive pause frames to on, off, or desired. The default state is off.

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.

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.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface</td>
<td>Identifies the interface type, the switch number (only on stacking-capable switches), and the number of the connector.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action: `Switch(config-if)#`

**Purpose**

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 0/1`, `gigabitethernet0/1`, `gi 0/1`, or `gi0/1`.

### Step 4

Follow each `interface` command with the interface configuration commands that the interface requires.

**Purpose**

Defines the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter `end` to return to privileged EXEC mode.

### Step 5

**Command or Action**

- `interface range`
- `interface range macro`

**Purpose**

(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

**Command or Action**

- `show interfaces`

**Purpose**

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

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `description string`
5. `end`
6. `show interfaces interface-id description`
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><code>interface interface-id</code>&lt;br&gt;Example: Switch(config)# interface gigabitethernet 0/2</td>
<td>Specifies the interface for which you are adding a description, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>description string</code>&lt;br&gt;Example: Switch(config-if)# description Connects to Marketing</td>
<td>Adds a description (up to 240 characters) for an interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code>&lt;br&gt;Example: Switch(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show interfaces interface-id description</code></td>
<td>Verifies your entry.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>copy running-config startup-config</code>&lt;br&gt;Example: Switch# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### 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.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface range {port-range | macro macro_name}`
4. `end`
5. `show interfaces [interface-id]`
6. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code>&lt;br&gt;Example:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface range {port-range</td>
<td>macro macro_name}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface range macro</td>
<td>• You can use the interface range command to configure up to five port ranges or a previously defined macro.</td>
</tr>
<tr>
<td></td>
<td>• The macro variable is explained in the Configuring and Using Interface Range Macros, on page 13.</td>
</tr>
<tr>
<td></td>
<td>• In a comma-separated port-range, you must enter the interface type for each entry and enter spaces before and after the comma.</td>
</tr>
<tr>
<td></td>
<td>• In a hyphen-separated port-range, you do not need to re-enter the interface type, but you must enter a space before the hyphen.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Use the normal configuration commands to apply the configuration parameters to all interfaces in the range. Each command is executed as it is entered.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show interfaces [interface-id]</td>
<td>Verifies the configuration of the interfaces in the range.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show interfaces</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
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.

SUMMARY STEPS

1. enable
2. configure terminal
3. define interface-range macro_name interface-range
4. interface range macro macro_name
5. end
6. show running-config | include define
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3 define interface-range macro_name interface-range</td>
<td>Defines the interface-range macro, and save it in NVRAM.</td>
</tr>
<tr>
<td>Example:</td>
<td>• The macro_name is a 32-character maximum character string.</td>
</tr>
<tr>
<td>Switch(config)# define interface-range enet_list 0/1 - 2</td>
<td>• A macro can contain up to five comma-separated interface ranges.</td>
</tr>
<tr>
<td></td>
<td>• Each interface-range must consist of the same port type.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4 interface range macro macro_name</td>
<td>Selects the interface range to be configured using the values saved in the interface-range macro called macro_name.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Ethernet Interfaces

Setting the Interface Speed and Duplex Parameters

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `speed {10 | 100 | 1000}`
5. `duplex {auto | full | half}`
6. `end`
7. `show interfaces interface-id`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

---

### Purpose

**Command or Action**

`Switch(config)# interface range macro enet_list`

You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.

**Step 5**

**Example:**

`Switch(config)# end`

Returns to privileged EXEC mode.

**Step 6**

**Example:**

`Switch# show running-config | include define`

Shows the defined interface range macro configuration.

**Step 7**

**Example:**

`Switch# copy running-config startup-config`

(Optional) Saves your entries in the configuration file.

---

**Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)**
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 2    | configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode. |
| 3    | interface interface-id  
Example:  
Switch(config)# interface gigabitethernet 0/3 | Specifies the physical interface to be configured, and enter interface configuration mode. |
| 4    | speed {10 | 100 | 1000}  
Example:  
Switch(config-if)# speed 10 | Enter the appropriate speed parameter for the interface:  
- Enter 10, 100, 1000 to set a specific speed for the interface. |
| 5    | duplex {auto | full | half}  
Example:  
Switch(config-if)# duplex half | This command is not available on a 10-Gigabit Ethernet interface.  
Enter the duplex parameter for the interface.  
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.  
You can configure the duplex setting when the speed is set to auto. |
| 6    | end  
Example:  
Switch(config-if)# end | Returns to privileged EXEC mode. |
| 7    | show interfaces interface-id  
Example:  
Switch# show interfaces gigabitethernet 0/3 | Displays the interface speed and duplex mode configuration. |
| 8    | copy running-config startup-config  
Example:  
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
## Configuring IEEE 802.3x Flow Control

### SUMMARY STEPS

1. `configure terminal`
2. `interface interface-id`
3. `flowcontrol {receive} {on | off | desired}`
4. `end`
5. `show interfaces interface-id`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode</td>
</tr>
</tbody>
</table>

| **Step 2** | interface interface-id |
| Example: | Switch(config)# interface gigabitethernet 0/1 |
| | Specifies the physical interface to be configured, and enter interface configuration mode. |

| **Step 3** | flowcontrol {receive} {on | off | desired} |
| Example: | Switch(config-if)# flowcontrol receive on |
| | Configures the flow control mode for the port. |

| **Step 4** | end |
| Example: | Switch(config-if)# end |
| | Returns to privileged EXEC mode. |

| **Step 5** | show interfaces interface-id |
| Example: | Switch# show interfaces gigabitethernet 0/1 |
| | Verifies the interface flow control settings. |

| **Step 6** | copy running-config startup-config |
| Example: | Switch# copy running-config startup-config |
| | (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.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface {vlan vlan-id} | {gigabitethernet interface-id} | {port-channel port-channel-number}`
4. `shutdown`
5. `no shutdown`
6. `end`
7. `show running-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`interface {vlan vlan-id}</td>
<td>{gigabitethernet interface-id}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 0/2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>shutdown</code></td>
<td>Shuts down an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# shutdown</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>no shutdown</code></td>
<td>Restarts an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# no shutdown</code></td>
<td></td>
</tr>
</tbody>
</table>
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.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `line console 0`
4. `media-type rj45`
5. `end`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>line console 0</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the console and enters line configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
**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.

---

**Note**

The configured inactivity timeout applies to all switches in a stack. However, a timeout on one switch does not cause a timeout on other switches in the stack.

### SUMMARY STEPS

1. enable
2. configure terminal
3. line console 0
4. usb-inactivity-timeout *timeout-minutes*
5. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
## 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 2: Show Commands for Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces interface-number downshift</code></td>
<td>Displays the downshift status details of the specified interfaces and modules.</td>
</tr>
<tr>
<td><code>module module-number</code></td>
<td></td>
</tr>
<tr>
<td><code>show interfaces interface-id status</code></td>
<td>Displays interface status or a list of interfaces in the error-disabled state.</td>
</tr>
<tr>
<td><code>[err-disabled]</code></td>
<td></td>
</tr>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>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.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><code>show interfaces [interface-id] description</code></td>
<td>Displays the description configured on an interface or all interfaces and the interface status.</td>
</tr>
<tr>
<td><code>show ip interface [interface-id]</code></td>
<td>Displays the usability status of all interfaces configured for IP routing or the specified interface.</td>
</tr>
<tr>
<td><code>show interface [interface-id] stats</code></td>
<td>Displays the input and output packets by the switching path for the interface.</td>
</tr>
<tr>
<td><code>show interfaces interface-id</code></td>
<td>(Optional) Displays speed and duplex on the interface.</td>
</tr>
<tr>
<td><code>show interfaces transceiver dom-supported-list</code></td>
<td>(Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules.</td>
</tr>
<tr>
<td><code>show interfaces transceiver properties</code></td>
<td>(Optional) Displays temperature, voltage, or amount of current on the interface.</td>
</tr>
<tr>
<td>`show interfaces [interface-id] [transceiver properties</td>
<td>detail] module number`</td>
</tr>
<tr>
<td><code>show running-config interface [interface-id]</code></td>
<td>Displays the running configuration in RAM for the interface.</td>
</tr>
<tr>
<td><code>show version</code></td>
<td>Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.</td>
</tr>
<tr>
<td><code>show controllers ethernet-controller interface-id phy</code></td>
<td>Displays the operational state of the auto-MDIX feature on the interface.</td>
</tr>
</tbody>
</table>

### Clearing and Resetting Interfaces and Counters

**Table 3: Clear Commands for Interfaces**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear counters [interface-id]</code></td>
<td>Clears interface counters.</td>
</tr>
<tr>
<td><code>clear interface interface-id</code></td>
<td>Resets the hardware logic on an interface.</td>
</tr>
<tr>
<td>`clear line [number</td>
<td>console 0</td>
</tr>
</tbody>
</table>

---

**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:

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

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:

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet 0/1 - 2
Switch(config)# end
Switch# show running-config | include define
define interface-range enet_list gigabitethernet 0/1 - 2
```

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

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

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

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

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:

```
Switch# configure terminal
```
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# speed 10
Switch(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:

Switch# configure terminal
Switch(config)# interface gigabitethernet 0/2
Switch(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.

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

This configuration terminates any active USB console media type in the stack. A log shows that this termination has occurred. This example shows that the console on switch 1 reverted to RJ-45.

*Mar 1 00:25:36.860: %USB_CONSOLE-6-CONFIG_DISABLE: Console media-type USB disabled by system configuration, media-type reverted to RJ45.

At this point no switches in the stack allow a USB console to have input. A log entry shows when a console cable is attached. If a USB console cable is connected to switch 2, it is prevented from providing input.

*Mar 1 00:34:27.498: %USB_CONSOLE-6-CONFIG_DISALLOW: Console media-type USB is disallowed by system configuration, media-type remains RJ45. (switch-stk-2)

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

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

Configuring the USB Inactivity Timeout: Example

This example configures the inactivity timeout to 30 minutes:

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

To disable the configuration, use these commands:

Switch# configure terminal
Switch(config)# line console 0
Switch(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

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
### Feature History and Information for Configuring Interface Characteristics

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Downshift on mGig interfaces: When port speed downshifting is enabled on an interface, the line rate automatically downgrades to a lower speed if the link quality is bad or if the link is continuously down. This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Auto-MDIX

- Prerequisites for Auto-MDIX, on page 27
- Restrictions for Auto-MDIX, on page 27
- Information about Configuring Auto-MDIX, on page 27
- How to Configure Auto-MDIX, on page 28
- Example for Configuring Auto-MDIX, on page 29
- Additional References, on page 30
- Feature History and Information for Auto-MDIX, on page 30

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 switch 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 switch 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 switches 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 switches 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 4: Link Conditions and Auto-MDIX Settings**

<table>
<thead>
<tr>
<th>Local Side Auto-MDIX</th>
<th>Remote Side Auto-MDIX</th>
<th>With Correct Cabling</th>
<th>With Incorrect Cabling</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>On</td>
<td>Link up</td>
<td>Link up</td>
</tr>
<tr>
<td>On</td>
<td>Off</td>
<td>Link up</td>
<td>Link up</td>
</tr>
<tr>
<td>Off</td>
<td>On</td>
<td>Link up</td>
<td>Link up</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>Link up</td>
<td>Link down</td>
</tr>
</tbody>
</table>

## How to Configure Auto-MDIX

### Configuring Auto-MDIX on an Interface

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `speed auto`
5. `duplex auto`
6. `end`
7. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode |
| Example:                     |                                   |
| Switch# configure terminal   |                                   |

<p>| <strong>Step 3</strong> interface interface-id | Specifies the physical interface to be configured, and enter interface configuration mode. |
| Example:                          |                                               |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td>Configure the interface to autonegotiate speed with the connected device.</td>
</tr>
<tr>
<td><strong>Step 4</strong> speed auto</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# speed auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> duplex auto</td>
<td>Configure the interface to autonegotiate duplex mode with the connected device.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# duplex auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Example for Configuring Auto-MDIX**

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

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

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for Auto-MDIX

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
</tbody>
</table>
Chapter 3

Configuring LLDP, LLDP-MED, and Wired Location Service

- Finding Feature Information, on page 31
- LLDP, LLDP-MED, and Wired Location Service Overview, on page 31
- How to Configure LLDP, LLDP-MED, and Wired Location Service, on page 34
- Configuration Examples for LLDP, LLDP-MED, and Wired Location Service, on page 42
- Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service, on page 42

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

LLDP, LLDP-MED, and Wired Location Service Overview

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 switch 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 Medianet

When you configure LLDP or CDP location information on a per-port basis, remote devices can send Cisco Medianet location information to the switch. For information, go to http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html.

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 such as switches. 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 switch, 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 switches 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 switch 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 switch 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 switch, 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 switch 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.

# Default LLDP Configuration

## Table 5: Default LLDP Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP global state</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP holdtime (before discarding)</td>
<td>120 seconds</td>
</tr>
<tr>
<td>LLDP timer (packet update frequency)</td>
<td>30 seconds</td>
</tr>
</tbody>
</table>
### 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 vlan-id` 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.

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

#### Enabling LLDP

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `lldp run`
4. `interface interface-id`
5. `lldp transmit`
6. `lldp receive`
7. `end`
8. `show lldp`
9. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example: Switch&gt; <strong>enable</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# <strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> lldp run</td>
<td>Enables LLDP globally on the switch.</td>
</tr>
<tr>
<td>Example: Switch (config)# <strong>lldp run</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface <strong>interface-id</strong></td>
<td>Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch (config)# <strong>interface gigabitethernet 0/1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> lldp transmit</td>
<td>Enables the interface to send LLDP packets.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <strong>lldp transmit</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> lldp receive</td>
<td>Enables the interface to receive LLDP packets.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <strong>lldp receive</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <strong>end</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> show lldp</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td>Example: Switch# <strong>show lldp</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
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.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. lldp holdtime seconds
4. lldp reinit delay
5. lldp timer rate
6. lldp tlv-select
7. interface interface-id
8. lldp med-tlv-select
9. end
10. show lldp
11. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| enable           | Enables privileged EXEC mode. |
| Example: Switch> enable | |
| **Step 2**
<p>| configure terminal | Enters global configuration mode. |
| Example: Switch# configure terminal | |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3    | lldp holdtime `seconds`  
Example: `Switch(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. |
| 4    | lldp reinit `delay`  
Example: `Switch(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. |
| 5    | lldp timer `rate`  
Example: `Switch(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. |
| 6    | lldp tlv-select  
Example: `Switch(config)# tlv-select` | (Optional) Specifies the LLDP TLVs to send or receive. |
| 7    | interface `interface-id`  
Example: `Switch (config)# interface gigabitethernet 0/1` | Specifies the interface on which you are enabling LLDP, and enter interface configuration mode. |
| 8    | lldp med-tlv-select  
Example: `Switch (config-if)# lldp med-tlv-select inventory management` | (Optional) Specifies the LLDP-MED TLVs to send or receive. |
| 9    | end  
Example: `Switch (config-if)# end` | Returns to privileged EXEC mode. |
| 10   | show lldp  
Example: `Switch# show lldp` | Verifies the configuration. |
**Configuring LLDP-MED TLVs**

By default, the switch 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>
<thead>
<tr>
<th>LLDP-MED TLV</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inventory-management</td>
<td>LLDP-MED inventory management TLV</td>
</tr>
<tr>
<td>location</td>
<td>LLDP-MED location TLV</td>
</tr>
<tr>
<td>network-policy</td>
<td>LLDP-MED network policy TLV</td>
</tr>
<tr>
<td>power-management</td>
<td>LLDP-MED power management TLV</td>
</tr>
</tbody>
</table>

Follow these steps to enable a TLV on an interface:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `lldp med-tlv-select`
5. `end`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Network-Policy TLV

**SUMMARY STEPS**

1. enable
2. configure terminal
3. network-policy profile profile number
4. {voice | voice-signaling} vlan [vlan-id {cos cvalue | dscp dvalue}] | [{dot1p | cos cvalue | dscp dvalue}] | none | untagged
5. exit
6. interface interface-id
7. network-policy profile number
8. lldp med-tlv-select network-policy
9. end
10. show network-policy profile

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 2    | configure terminal  
**Example:**  
Switch# configure terminal | Enters global configuration mode. |
| 3    | interface interface-id  
**Example:**  
Switch (config)# interface gigabitethernet 0/1 | Specifies the interface on which you are enabling LLDP, and enter interface configuration mode. |
| 4    | lldp med-tlv-select  
**Example:**  
Switch(config-if)# lldp med-tlv-select inventory management | Specifies the TLV to enable. |
| 5    | end  
**Example:**  
Switch(config-if)# end | Returns to privileged EXEC mode. |
| 6    | copy running-config startup-config  
**Example:**  
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
## Configuring Network-Policy TLV

### DETAILED STEPS

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

**Step 5**

```
exit
```

Returns to global configuration mode.

**Step 6**

```
interface interface-id
```

Specifies the interface on which you are configuring a network-policy profile, and enter interface configuration mode.

**Example:**

```
Switch(config)# interface gigabitethernet 0/1
```

**Step 7**

```
network-policy profile number
```

Specifies the network-policy profile number.

**Example:**

```
Switch(config-if)# network-policy 1
```

**Step 8**

```
lldp med-tlv-select network-policy
```

Specifies the network-policy TLV.

**Example:**

```
Switch(config-if)# lldp med-tlv-select network-policy
```

**Step 9**

```
end
```

Returns to privileged EXEC mode.

**Step 10**

```
show network-policy profile
```

Verifies the configuration.

**Example:**

```
Switch# show network-policy profile
```

**Step 11**

```
copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

**Example:**

```
Switch# copy running-config startup-config
```
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:

```
Switch# configure terminal
Switch(config)# network-policy 1
Switch(config-network-policy)# voice vlan 100 cos 4
Switch(config-network-policy)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# network-policy profile 1
Switch(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:

```
Switch(config-network-policy)# voice vlan dot1p cos 4
Switch(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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lldp counters</td>
<td>Resets the traffic counters to zero.</td>
</tr>
<tr>
<td>clear lldp table</td>
<td>Deletes the LLDP neighbor information table.</td>
</tr>
<tr>
<td>clear nmsp statistics</td>
<td>Clears the NMSP statistic counters.</td>
</tr>
<tr>
<td>show lldp</td>
<td>Displays global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time before LLDP initializes on an interface.</td>
</tr>
<tr>
<td>show lldp entry entry-name</td>
<td>Displays information about a specific neighbor.  You can enter an asterisk (*) to display all neighbors, or you can enter the neighbor name.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show lldp interface [interface-id]</code></td>
<td>Displays information about interfaces with LLDP enabled. You can limit the display to a specific interface.</td>
</tr>
<tr>
<td><code>show lldp neighbors [interface-id] [detail]</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>show lldp traffic</code></td>
<td>Displays LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.</td>
</tr>
<tr>
<td><code>show location admin-tag string</code></td>
<td>Displays the location information for the specified administrative tag or site.</td>
</tr>
<tr>
<td><code>show location civic-location identifier id</code></td>
<td>Displays the location information for a specific global civic location.</td>
</tr>
<tr>
<td><code>show location elin-location identifier id</code></td>
<td>Displays the location information for an emergency location.</td>
</tr>
<tr>
<td><code>show network-policy profile</code></td>
<td>Displays the configured network-policy profiles.</td>
</tr>
<tr>
<td><code>show nmsp</code></td>
<td>Displays the NMSP information</td>
</tr>
</tbody>
</table>
Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service
Configuring System MTU

- Finding Feature Information, on page 45
- Information About the MTU, on page 45
- How to Configure MTU, on page 45
- Configuration Examples for System MTU, on page 46

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces is 1500 bytes.

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:

SUMMARY STEPS

1. configure terminal
2. system mtu bytes
3. `system mtu jumbo`
4. `end`
5. `copy running-config startup-config`
6. `do show system mtu`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**        | Enters global configuration mode.  
  **Example:**  
  ```bash
  configure terminal
  ```  
  ```bash
  Switch# configure terminal
  ``` |
| **Step 2**        | (Optional) Change the MTU size for all interfaces on the switch stack that are operating at 10 or 100 Mb/s.  
  **Example:**  
  ```bash
  system mtu bytes
  ```  
  ```bash
  Switch(config)# system mtu 1500
  ``` |
| **Step 3**        | (Optional) Changes the MTU size for all Gigabit Ethernet interfaces on the switch or the switch stack.  
  **Example:**  
  ```bash
  system mtu jumbo
  ```  
  ```bash
  Switch(config)# system mtu jumbo
  ``` |
| **Step 4**        | Returns to privileged EXEC mode.  
  **Example:**  
  ```bash
  end
  ```  
  ```bash
  Switch(config)# end
  ``` |
| **Step 5**        | Saves your entries in the configuration file.  
  **Example:**  
  ```bash
  copy running-config startup-config
  ```  
  ```bash
  Switch# copy running-config startup-config
  ``` |
| **Step 6**        |  
  **Example:**  
  ```bash
  do show system mtu
  ```  
  ```bash
  Switch# do show system mtu
  ``` |

### Configuration Examples for System MTU

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 1500 bytes:

```bash
Switch(config)# system mtu 1500
Switch(config)# exit
```

This is an example of output from the `show system mtu` command:

```bash
Switch# show system mtu
```
System MTU size is 1500 bytes.
Configuration Examples for System MTU
CHAPTER 5

Configuring PoE
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for EEE

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.

EEE can be enabled on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

Default EEE Configuration

EEE is enabled by default.

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

SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. power efficient-ethernet auto
4. no power efficient-ethernet auto
5. end
6. copy running-config startup-config

DETAILED STEPS

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

### Monitoring EEE

#### Table 7: Commands for Displaying EEE Settings

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show eee capabilities interface interface-id</code></td>
<td>Displays EEE capabilities for the specified interface.</td>
</tr>
<tr>
<td><code>show eee status interface interface-id</code></td>
<td>Displays EEE status information for the specified interface.</td>
</tr>
<tr>
<td><code>show eee counters interface interface-id</code></td>
<td>Displays EEE counters for the specified interface.</td>
</tr>
</tbody>
</table>

**Note** This command is not supported on Catalyst Digital Building uplink ports in the Cisco IOS Release 15.2(6)2E

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

---

**Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)**
Switch# show eee capabilities interface gigabitEthernet0/1
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 gigabitEthernet0/1
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 gigabitEthernet0/1
LP Active Tx Time (10us): 66649648
LP Transitioning Tx: 462
LP Active Rx Time (10us): 64911682
LP Transitioning Rx: 153

Examples for Cataylst Digital Building Series Switches

Switch# show eee capabilities interface gig0/1
Gi1/0/1
EEE(efficient-ethernet): yes (100-Tx and 1000T auto)
Link Partner: no

Switch# show eee status int gig0/1
Gi1/0/1 is up
EEE(efficient-ethernet): Disagreed
Rx LPI Status: None
Tx LPI Status: None
Wake Error Count: 0

---

Configuration Examples for Configuring EEE

This example shows how to enable EEE for an interface:

Switch# configure terminal
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# power efficient-ethernet auto

This example shows how to disable EEE for an interface:

Switch# configure terminal
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# no power efficient-ethernet auto

---
### Additional References

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature History and Information for Configuring EEE

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
<tr>
<td>This feature was introduced.</td>
<td></td>
</tr>
</tbody>
</table>
PART II

IP Multicast Snooping

• Configuring IGMP Snooping, on page 59
• Configuring MLD Snooping, on page 97
CHAPTER 7

Configuring IGMP Snooping

• Finding Feature Information, on page 59
• Prerequisites for Configuring IGMP Snooping, on page 59
• Restrictions for Configuring IGMP Snooping, on page 60
• Information About IGMP Snooping, on page 61
• How to Configure IGMP Snooping, on page 66
• Monitoring IGMP Snooping, on page 90
• Configuration Examples for IGMP Snooping, on page 92
• Additional References, on page 94
• Feature History and Information for IGMP Snooping, on page 95

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring IGMP Snooping

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 switch virtual interface (SVI) IP address (if one exists). If there is no SVI
IP address, the switch uses the first available IP address configured on the switch. 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 switch.

- 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 if IGMP snooping is disabled in the VLAN.
- Layer 3 multicast is not supported.
- MAC based snooping is supported in hardware.

**Related Topics**
- Configuring the IGMP Snooping Querier, on page 80
- IGMP Snooping, on page 61

### Restrictions for Configuring IGMP Snooping

### 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 switches 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 switch.

  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.
Information About IGMP Snooping

IGMP Snooping

Layer 2 switches 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 switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch 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.

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 switch 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 switch 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 switch 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:

Related Topics
  Configuring the IGMP Snooping Querier, on page 80
IGMP Versions

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

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

Related Topics
- Restrictions for IGMP Snooping, on page 60

Joining a Multicast Group

When a host connected to the switch 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 switch 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 switch. The switch 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 switch, 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 switch 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 8: IGMP Snooping Forwarding Table

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2</td>
</tr>
</tbody>
</table>

The switch 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 3: 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 switch. Any known multicast traffic is forwarded to the group and not to the CPU.

Table 9: Updated IGMP Snooping Forwarding Table

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Type of Packet</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.2.3</td>
<td>IGMP</td>
<td>1, 2, 5</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring a Host Statically to Join a Group, on page 72
- Example: Configuring a Host Statically to Join a Group, on page 92

Leaving a Multicast Group

The router sends periodic multicast general queries, and the switch 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 switch 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 switch 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 switch 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 switch uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends
a leave message without the switch 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
switch.

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.

Related Topics

Enabling IGMP Immediate Leave, on page 73
Example: Enabling IGMP Immediate Leave, on page 92

IGMP Configurable-Leave Timer

You can configure the time that the switch 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.

Related Topics

Configuring the IGMP Leave Timer, on page 74

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 switch 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 switch sends the first IGMP
report from all hosts for a group to all the multicast routers. The switch 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 switch 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 switch 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.
Default IGMP Snooping Configuration

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

Table 10: Default IGMP Snooping Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping</td>
<td>Enabled globally and per VLAN</td>
</tr>
<tr>
<td>Multicast routers</td>
<td>None configured</td>
</tr>
<tr>
<td>IGMP snooping Immediate Leave</td>
<td>Disabled</td>
</tr>
<tr>
<td>Static groups</td>
<td>None configured</td>
</tr>
<tr>
<td>TCN(^1) flood query count</td>
<td>2</td>
</tr>
<tr>
<td>TCN query solicitation</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP snooping querier</td>
<td>Disabled</td>
</tr>
<tr>
<td>IGMP report suppression</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

\(^1\) (1) TCN = Topology Change Notification

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 switch 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 switch 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 switch 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 switch 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 switches running IGMP filtering.

**Related Topics**

- Configuring IGMP Profiles, on page 83
- Applying IGMP Profiles, on page 85
- Setting the Maximum Number of IGMP Groups, on page 87
- Configuring the IGMP Throttling Action, on page 88
- Restrictions for IGMP Snooping, on page 60

### Default IGMP Filtering and Throttling Configuration

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

**Table 11: Default IGMP Filtering Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP filters</td>
<td>None applied.</td>
</tr>
<tr>
<td>IGMP maximum number of IGMP groups</td>
<td>No maximum set.</td>
</tr>
<tr>
<td>Note</td>
<td>When the maximum number of groups is in the forwarding table, the default IGMP throttling action is to deny the IGMP report.</td>
</tr>
<tr>
<td>IGMP profiles</td>
<td>None defined.</td>
</tr>
<tr>
<td>IGMP profile action</td>
<td>Deny the range addresses.</td>
</tr>
</tbody>
</table>

### How to Configure IGMP Snooping

#### Enabling or Disabling IGMP Snooping on a Switch

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 switch:
SUMMARY STEPS

1. enable
2. configure terminal
3. ip igmp snooping
4. end
5. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip igmp snooping</td>
<td>Globally enables IGMP snooping in all existing VLAN interfaces.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: To globally disable IGMP snooping on all VLAN interfaces, use the no ip igmp snooping global configuration command.</td>
</tr>
<tr>
<td>Switch(config)# ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
Default IGMP Snooping Configuration, on page 65

Enabling or Disabling IGMP Snooping on a VLAN Interface

Follow these steps to enable IGMP snooping on a VLAN interface:
Enabling or Disabling IGMP Snooping on a VLAN Interface

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip igmp snooping vlan vlan-id`
4. `end`
5. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; <code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip igmp snooping vlan vlan-id</code></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>ip igmp snooping vlan 7</code></td>
<td>Note: To disable IGMP snooping on a VLAN interface, use the <strong>no ip igmp snooping vlan vlan-id</strong> global configuration command for the specified VLAN number.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

[Default IGMP Snooping Configuration](#), on page 65
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.

Note
Static connection using the `ip igmp snooping mrouter` command is supported only for known multicast groups.

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.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip igmp snooping vlan vlan-id mrouter learn {cgmp | pim-dvmrp}
4. end
5. show ip igmp snooping
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Multicast Router Port

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

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

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip igmp snooping vlan \(vlan-id\) mrouter interface interface-id
4. end
5. `show ip igmp snooping mrouter [vlan vlan-id]`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
| **Example:**
| `Switch>` `enable` |
| **Step 2** | Enters global configuration mode. |
| `configure terminal` | |
| **Example:**
| `Switch# configure terminal` |
| **Step 3** | Specifies the multicast router VLAN ID and the interface to the multicast router. |
| `ip igmp snooping vlan vlan-id mrouter interface interface-id` | • The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| **Example:**
| `Switch(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet0/1` | • The interface can be a physical interface or a port channel. The port-channel range is 1 to 128. |
| **Note** | To remove a multicast router port from the VLAN, use the `no ip igmp snooping vlan vlan-id mrouter interface interface-id` global configuration command. |
| **Step 4** | Returns to privileged EXEC mode. |
| `end` | |
| **Example:**
| `Switch(config)# end` |
| **Step 5** | Verifies that IGMP snooping is enabled on the VLAN interface. |
| `show ip igmp snooping mrouter [vlan vlan-id]` | |
| **Example:**
| `Switch# show ip igmp snooping mrouter vlan 5` |
| **Step 6** | (Optional) Saves your entries in the configuration file. |
| `copy running-config startup-config` | |
| **Example:**
| `Switch# copy running-config startup-config` |
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:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip igmp snooping vlan vlan-id static ip_address interface interface-id`
4. `end`
5. `show ip igmp snooping groups`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>ip igmp snooping vlan vlan-id static ip_address interface interface-id</code></td>
<td>Synchronously configures a Layer 2 port as a member of a multicast group:</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note** To remove the Layer 2 port from the multicast group, use the `no ip igmp snooping vlan vlan-id static mac-address interface interface-id` global configuration command.
### Related Topics

- [Joining a Multicast Group](#), on page 62
- [Example: Configuring a Host Statically to Join a Group](#), on page 92

### Enabling IGMP Immediate Leave

When you enable IGMP Immediate Leave, the switch 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 switch.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip igmp snooping vlan vlan-id immediate-leave`
4. `end`
5. `show ip igmp snooping vlan vlan-id`
6. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### 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:

**SUMMARY STEPS**

1. enable
2. configure terminal

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Step 2**

**configure terminal**

**Example:**

Switch# configure terminal

**Purpose:** Enters global configuration mode.

**Step 3**

**ip igmp snooping vlan vlan-id immediate-leave**

**Example:**

Switch(config)# ip igmp snooping vlan 21 immediate-leave

**Purpose:** Enables IGMP Immediate Leave on the VLAN interface.

**Note:** To disable IGMP Immediate Leave on a VLAN, use the `no ip igmp snooping vlan vlan-id immediate-leave` global configuration command.

**Step 4**

**end**

**Example:**

Switch(config)# end

**Purpose:** Returns to privileged EXEC mode.

**Step 5**

**show ip igmp snooping vlan vlan-id**

**Example:**

Switch# show ip igmp snooping vlan 21

**Purpose:** Verifies that Immediate Leave is enabled on the VLAN interface.

**Step 6**

**end**

**Example:**

Switch(config)# end

**Purpose:** Returns to privileged EXEC mode.

---

**Related Topics**

- Immediate Leave, on page 64
- Example: Enabling IGMP Immediate Leave, on page 92
### IP Multicast Snooping

3. `ip igmp snooping last-member-query-interval time`
4. `ip igmp snooping vlan vlan-id last-member-query-interval time`
5. `end`
6. `show ip igmp snooping`
7. `copy running-config startup-config`

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>ip igmp snooping last-member-query-interval time</code></td>
<td>Configures the IGMP leave timer globally. The range is 100 to 32767 milliseconds.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ip igmp snooping last-member-query-interval 1000</td>
<td>The default leave time is 1000 milliseconds.</td>
</tr>
<tr>
<td><strong>Note</strong> To globally reset the IGMP leave timer to the default setting, use the <code>no ip igmp snooping last-member-query-interval</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip igmp snooping vlan vlan-id last-member-query-interval time</code></td>
<td>(Optional) Configures the IGMP leave time on the VLAN interface. The range is 100 to 32767 milliseconds.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ip igmp snooping vlan 210 last-member-query-interval 1000</td>
<td><strong>Note</strong> Configuring the leave time on a VLAN overrides the globally configured timer.</td>
</tr>
<tr>
<td><strong>Note</strong> To remove the configured IGMP leave-time setting from the specified VLAN, use the <code>no ip igmp snooping vlan vlan-id last-member-query-interval</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring TCN-Related Commands

#### Controlling the Multicast Flooding Time After a TCN Event

You can configure the number of general queries by which multicast data traffic is flooded after a topology change notification (TCN) event. If you set the TCN flood query count to 1 the flooding stops after receiving 1 general query. If you set the count to 7, the flooding continues until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Some examples of TCN events are when the client location is changed and the receiver is on same port that was blocked but is now forwarding, and when a port goes down without sending a leave message.

Follow these steps to configure the TCN flood query count:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip igmp snooping tcn flood query count count`
4. `end`
5. `show ip igmp snooping`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
</tr>
</tbody>
</table>

Enables privileged EXEC mode.

- Enter your password if prompted.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip igmp snooping tcn flood query count</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show ip igmp snooping</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
</tbody>
</table>

### Recovering from Flood Mode

When a topology change occurs, the spanning-tree root sends a special IGMP leave message (also known as global leave) with the group multicast address 0.0.0.0. However, you can enable the switch to send the global leave message whether it is the spanning-tree root or not. When the router receives this special leave, it immediately sends general queries, which expedite the process of recovering from the flood mode during the TCN event. Leaves are always sent if the switch is the spanning-tree root regardless of this configuration.

Follow these steps to enable sending of leave messages:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip igmp snooping tcn query solicit`
4. `end`
5. show ip igmp snooping
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ip igmp snooping tcn query solicit</td>
<td>Sends an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event. By default, query solicitation is disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note</td>
</tr>
<tr>
<td>Switch(config)# ip igmp snooping tcn query solicit</td>
<td>To return to the default query solicitation, use the <strong>no ip igmp snooping tcn query solicit</strong> global configuration command.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>show ip igmp snooping</td>
<td>Verifies the TCN settings.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip igmp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Disabling Multicast Flooding During a TCN Event**

When the switch receives a TCN, multicast traffic is flooded to all the ports until 2 general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding might exceed the capacity of the link and cause packet loss. Follow these steps to control TCN flooding:
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. no ip igmp snooping tcn flood
5. end
6. show ip igmp snooping
7. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the interface to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no ip igmp snooping tcn flood</td>
<td>Disables the flooding of multicast traffic during a spanning-tree TCN event.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# no ip igmp snooping tcn flood</td>
<td>By default, multicast flooding is enabled on an interface.</td>
</tr>
<tr>
<td>Note</td>
<td>To re-enable multicast flooding on an interface, use the <strong>ip igmp snooping tcn flood</strong> interface configuration command.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show ip igmp snooping</td>
<td>Verifies the TCN settings.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the IGMP Snooping Querier

Follow these steps to enable the IGMP snooping querier feature in a VLAN:

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip igmp snooping querier**
4. **ip igmp snooping querier address ip_address**
5. **ip igmp snooping querier query-interval interval-count**
6. **ip igmp snooping querier tcn query [count count | interval interval]**
7. **ip igmp snooping querier timer expiry timeout**
8. **ip igmp snooping querier version version**
9. **end**
10. **show ip igmp snooping vlan vlan-id**
11. **copy running-config startup-config**

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip igmp snooping querier</td>
<td>Enables the IGMP snooping querier.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# ip igmp snooping querier</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# ip igmp snooping querier</code></td>
<td><strong>Step 4</strong> Specifies an IP address for the IGMP snooping querier. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier. <strong>Note</strong> The IGMP snooping querier does not generate an IGMP general query if it cannot find an IP address on the switch.</td>
</tr>
<tr>
<td><code>ip igmp snooping querier address ip_address</code></td>
<td>(Optional) Sets the interval between IGMP queries. The range is 1 to 18000 seconds.</td>
</tr>
<tr>
<td><code>ip igmp snooping querier query-interval interval-count</code></td>
<td>(Optional) Sets the interval between IGMP queries. The range is 1 to 18000 seconds.</td>
</tr>
<tr>
<td>`ip igmp snooping querier tcn query [count count</td>
<td>interval interval]`</td>
</tr>
<tr>
<td><code>ip igmp snooping querier timer expiry timeout</code></td>
<td>(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.</td>
</tr>
<tr>
<td><code>ip igmp snooping querier version version</code></td>
<td>(Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)**
### Command or Action

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show IP IGMP Snooping VLAN</td>
<td><strong>show ip igmp snooping vlan vlan-id</strong>&lt;br&gt;Example:&lt;br&gt;<code>Switch# show ip igmp snooping vlan 30</code></td>
<td>(Optional) Verifies that the IGMP snooping querier is enabled on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Step 11</td>
<td><strong>copy running-config startup-config</strong>&lt;br&gt;Example:&lt;br&gt;<code>Switch# copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Related Topics
- **IGMP Snooping**, on page 61
- **Prerequisites for IGMP Snooping**, on page 59
- Example: Setting the IGMP Snooping Querier Source Address, on page 92
- Example: Setting the IGMP Snooping Querier Maximum Response Time, on page 93
- Example: Setting the IGMP Snooping Querier Timeout, on page 93
- Example: Setting the IGMP Snooping Querier Feature, on page 93

### Disabling IGMP Report Suppression

Follow these steps to disable IGMP report suppression:

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **no ip igmp snooping report-suppression**
4. **end**
5. **show ip igmp snooping**
6. **copy running-config startup-config**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;Example:&lt;br&gt;<code>Switch&gt; enable</code></td>
</tr>
<tr>
<td><strong>Enables privileged EXEC mode.</strong>&lt;br&gt;* Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Example:</td>
</tr>
<tr>
<td><strong>Enters global configuration mode.</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command or Action</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
</tr>
</tbody>
</table>

### Step 3

**no ip igmp snooping report-suppression**

**Example:**

```
Switch(config)# no ip igmp snooping report-suppression
```

To re-enable IGMP report suppression, use the `ip igmp snooping report-suppression` global configuration command.

### Step 4

**end**

**Example:**

```
Switch(config)# end
```

Returns to privileged EXEC mode.

### Step 5

**show ip igmp snooping**

**Example:**

```
Switch# show ip igmp snooping
```

Verifies that IGMP report suppression is disabled.

### Step 6

**copy running-config startup-config**

**Example:**

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

### Related Topics

- IGMP Report Suppression, on page 64

### Configuring IGMP Profiles

Follow these steps to create an IGMP profile:

This task is optional.

### SUMMARY STEPS

1. enable
2. configure terminal
3. ip igmp profile *profile number*
4. permit | deny
### Configuring IGMP Profiles

5. `range ip multicast address`  
6. `end`  
7. `show ip igmp profile profile number`  
8. `show running-config`  
9. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Steps</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
**Example:**  
Switch> `enable`  
| | `configure terminal` | Enters global configuration mode.  
**Example:**  
Switch# `configure terminal`  
| **Step 3** | `ip igmp profile profile number` | Assigns a number to the profile you are configuring, and enters IGMP profile configuration mode. The profile number range is 1 to 4294967295. When you are in IGMP profile configuration mode, you can create the profile by using these commands:  
**Example:**  
Switch(config)# `ip igmp profile 3`  
| | `permit` | (Optional) Sets the action to permit or deny access to the IP multicast address. If no action is configured, the default for the profile is to deny access.  
**Example:**  
Switch(config-igmp-profile)# `permit`  

#### Note: To delete a profile, use the `no ip igmp profile profile number` global configuration command.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** | **range ip multicast address**  
Example:  
Switch(config-igmp-profile)# range 229.9.9.0 | Enters the IP multicast address or range of IP multicast addresses to which access is being controlled. If entering a range, enter the low IP multicast address, a space, and the high IP multicast address.  
You can use the `range` command multiple times to enter multiple addresses or ranges of addresses.  
**Note** To delete an IP multicast address or range of IP multicast addresses, use the `no range ip multicast address` IGMP profile configuration command. |
| **Step 6** | **end**  
Example:  
Switch(config)# end | Returns to privileged EXEC mode. |
| **Step 7** | **show ip igmp profile profile number**  
Example:  
Switch# show ip igmp profile 3 | Verifies the profile configuration. |
| **Step 8** | **show running-config**  
Example:  
Switch# show running-config | Verifies your entries. |
| **Step 9** | **copy running-config startup-config**  
Example:  
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

**Related Topics**  
- IGMP Filtering and Throttling, on page 65  
- Restrictions for IGMP Snooping, on page 60

### Applying IGMP Profiles

To control access as defined in an IGMP profile, you have to apply the profile to the appropriate interfaces. You can apply IGMP profiles only to Layer 2 access ports; you cannot apply IGMP profiles to routed ports or SVIs. You cannot apply profiles to ports that belong to an EtherChannel port group. You can apply a profile to multiple interfaces, but each interface can have only one profile applied to it.

Follow these steps to apply an IGMP profile to a switch port:
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `ip igmp filter profile number`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface <code>interface-id</code></td>
<td>Specifies the physical interface, and enters interface configuration mode. The interface must be a Layer 2 port that does not belong to an EtherChannel port group.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip igmp filter profile number</code></td>
<td>Applies the specified IGMP profile to the interface. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip igmp filter 321</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>
### Setting the Maximum Number of IGMP Groups

Follow these steps to set the maximum number of IGMP groups that a Layer 2 interface can join:

#### Before you begin

This restriction can be applied to Layer 2 ports only; you cannot set a maximum number of IGMP groups on routed ports or SVIs. You also can use this command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `ip igmp max-groups number`
5. `end`
6. `show running-config interface interface-id`
7. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**Related Topics**
- IGMP Filtering and Throttling, on page 65
- Restrictions for IGMP Snooping, on page 60

---

### Purpose

Command or Action: `copy running-config startup-config`  
(Optional) Saves your entries in the configuration file.

**Example:**

```
Switch# copy running-config startup-config
```
### Configuring the IGMP Throttling Action

After you set the maximum number of IGMP groups that a Layer 2 interface can join, you can configure an interface to replace the existing group with the new group for which the IGMP report was received.

Follow these steps to configure the throttling action when the maximum number of entries is in the forwarding table:

### SUMMARY STEPS

1. enable
2. configure terminal

---

### Command or Action | Purpose |
--- | --- |
**Step 3** | **interface interface-id** | Specifies the interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or a EtherChannel interface.

**Example:**

Switch(config)# interface gigabitethernet0/2

**Step 4** | **ip igmp max-groups number** | Sets the maximum number of IGMP groups that the interface can join. The range is 0 to 4294967294. The default is to have no maximum set.

**Example:**

Switch(config-if)# ip igmp max-groups 20

**Note** To remove the maximum group limitation and return to the default of no maximum, use the **no ip igmp max-groups** interface configuration command.

**Step 5** | **end** | Returns to privileged EXEC mode.

**Example:**

Switch(config)# end

**Step 6** | **show running-config interface interface-id** | Verifies your entries.

**Example:**

Switch# interface gigabitethernet0/1

**Step 7** | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file.

**Example:**

Switch# copy running-config startup-config

---

**Related Topics**

- IGMP Filtering and Throttling, on page 65
- Restrictions for IGMP Snooping, on page 60
3. `interface interface-id`
4. `ip igmp max-groups action {deny | replace}`
5. `end`
6. `show running-config interface interface-id`
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the physical interface to be configured, and enters interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or an EtherChannel interface. The interface cannot be a trunk port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip igmp max-groups action {deny</td>
<td>replace}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip igmp max-groups action replace</td>
<td>• deny—Drops the report. If you configure this throttling action, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out and the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• replace—Replaces the existing group with the new group for which the IGMP report was received. If you configure this throttling action, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly selected entry with the received IGMP report.</td>
</tr>
<tr>
<td></td>
<td>To prevent the switch from removing the forwarding-table entries, you can configure the IGMP throttling action before an interface adds entries to the forwarding table.</td>
</tr>
</tbody>
</table>
To return to the default action of dropping the report, use the `no ip igmp max-groups` action interface configuration command.

### Step 5

**Purpose**

Returns to privileged EXEC mode.

**Example:**

```
Step 5
Switch(config)# end
```

### Step 6

**Purpose**

Verifies your entries.

**Example:**

```
Step 6
Switch# show running-config interface gigabitethernet0/1
```

### Step 7

**Purpose**

(Optional) Saves your entries in the configuration file.

**Example:**

```
Step 7
Switch# copy running-config startup-config
```

### Related Topics

- IGMP Filtering and Throttling, on page 65
- Restrictions for IGMP Snooping, on page 60

## Monitoring IGMP Snooping

### Monitoring IGMP Snooping Information

You can display IGMP snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display MAC address multicast entries for a VLAN configured for IGMP snooping.

**Table 12: Commands for Displaying IGMP Snooping Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip igmp snooping [vlan vlan-id [detail]]</code></td>
<td>Displays the snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>
Purpose

### Command

**show ip igmp snooping groups [count | vlan vlan-id]**

Displays multicast table information for the switch or about a specific parameter:

- **count**—Displays the total number of entries for the specified command options instead of the actual entries.
- **vlan-id**—The VLAN ID range is 1 to 1001 and 1006 to 4094.

**show ip igmp snooping mroutert [vlan vlan-id]**

Displays information on dynamically learned and manually configured multicast router interfaces.

**show ip igmp snooping querier [vlan vlan-id] detail**

Displays information about the IP address and receiving port of the most-recently received IGMP query message in the VLAN and the configuration and operational state of the IGMP snooping querier in the VLAN.

### Monitoring IGMP Filtering

You can display IGMP profile characteristics, and you can display the IGMP profile and maximum group configuration for all interfaces on the switch or for a specified interface.

**Table 13: Commands for Displaying IGMP Filtering**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip igmp profile [profile number]</strong></td>
<td>Displays the specified IGMP profile or all the IGMP profiles defined on the switch.</td>
</tr>
<tr>
<td><strong>show running-config [interface interface-id]</strong></td>
<td>Displays the configuration of the specified interface or the configuration of all interfaces on the switch, including (if configured) the maximum number of IGMP groups to which an interface can belong and the IGMP profile applied to the interface.</td>
</tr>
</tbody>
</table>
Configuration Examples for IGMP Snooping

Example: Configuring IGMP Snooping Using CGMP Packets

This example shows how to configure IGMP snooping to use CGMP packets as the learning method:

Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end

Example: Enabling a Static Connection to a Multicast Router

This example shows how to enable a static connection to a multicast router:

Switch configure terminal
Switch ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch end

Related Topics

Configuring a Multicast Router Port, on page 70

Example: Configuring a Host Statically to Join a Group

This example shows how to statically configure a host on a port:

Switch# configure terminal
Switch# ip igmp snooping vlan 105 static 0100.1212.0000 interface gigabitethernet0/1
Switch# end

Related Topics

Configuring a Host Statically to Join a Group, on page 72
Joining a Multicast Group, on page 62

Example: Enabling IGMP Immediate Leave

This example shows how to enable IGMP Immediate Leave on VLAN 130:

Switch# configure terminal
Switch(config)# ip igmp snooping vlan 130 immediate-leave
Switch(config)# end

Related Topics

Enabling IGMP Immediate Leave, on page 73
Immediate Leave, on page 64

Example: Setting the IGMP Snooping Querier Source Address

This example shows how to set the IGMP snooping querier source address to 10.0.0.64:
Example: Setting the IGMP Snooping Querier Maximum Response Time

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

Switch# configure terminal
Switch(config)# ip igmp snooping querier query-interval 25
Switch(config)# end

Example: Setting the IGMP Snooping Querier Timeout

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

Switch# configure terminal
Switch(config)# ip igmp snooping querier timeout expiry 60
Switch(config)# end

Example: Setting the IGMP Snooping Querier Feature

This example shows how to set the IGMP snooping querier feature to Version 2:

Switch# configure terminal
Switch(config)# no ip igmp snooping querier version 2
Switch(config)# end

Example: Configuring IGMP Profiles

This example shows how to create IGMP profile 4 allowing access to the single IP multicast address and how to verify the configuration. If the action was to deny (the default), it would not appear in the show ip igmp profile output display.

Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Example: Applying IGMP Profile

This example shows how to apply IGMP profile 4 to a port:

```bash
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

Example: Setting the Maximum Number of IGMP Groups

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```bash
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>IGMP Snooping and MVR Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 2960-X Switch)</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1112</td>
<td>Host Extensions for IP Multicasting</td>
</tr>
<tr>
<td>RFC 2236</td>
<td>Internet Group Management Protocol, Version 2</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for IGMP Snooping

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
<tr>
<td>This feature was introduced.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring MLD Snooping

This module contains details of configuring MLD snooping

- Finding Feature Information, on page 97
- Information About Configuring IPv6 MLD Snooping, on page 97
- How to Configure IPv6 MLD Snooping, on page 100
- Displaying MLD Snooping Information, on page 108
- Configuration Examples for Configuring MLD Snooping, on page 109

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring IPv6 MLD Snooping

You can use Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP Version 6 (IPv6) multicast data to clients and routers in a switched network on the switch.

Understanding MLD Snooping

In IP Version 4 (IPv4), Layer 2 switches can use Internet Group Management Protocol (IGMP) snooping to limit 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. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on the links that are directly attached to the routers and to discover which
multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD Version 1 (MLDv1) is equivalent to IGMPv2, and MLD Version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol Version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

The switch supports two versions of MLD snooping:

- MLDv1 snooping detects MLDv1 control packets and sets up traffic bridging based on IPv6 destination multicast addresses.
- MLDv2 basic snooping (MBSS) uses MLDv2 control packets to set up traffic forwarding based on IPv6 destination multicast addresses.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast addresses.

---

**Note**

The switch does not support MLDv2 enhanced snooping, which sets up IPv6 source and destination multicast address-based forwarding.

MLD snooping can be enabled or disabled globally or per VLAN. When MLD snooping is enabled, a per-VLAN IPv6 multicast address table is constructed in software and hardware. The switch then performs IPv6 multicast-address based bridging in hardware.

### MLD Messages

MLDv1 supports three types of messages:

- Listener Queries are the equivalent of IGMPv2 queries and are either General Queries or Multicast-Address-Specific Queries (MASQs).
- Multicast Listener Reports are the equivalent of IGMPv2 reports
- Multicast Listener Done messages are the equivalent of IGMPv2 leave messages.

MLDv2 supports MLDv2 queries and reports, as well as MLDv1 Report and Done messages.

Message timers and state transitions resulting from messages being sent or received are the same as those of IGMPv2 messages. MLD messages that do not have valid link-local IPv6 source addresses are ignored by MLD routers and switches.

### MLD Queries

The switch sends out MLD queries, constructs an IPv6 multicast address database, and generates MLD group-specific and MLD group-and-source-specific queries in response to MLD Done messages. The switch also supports report suppression, report proxying, Immediate-Leave functionality, and static IPv6 multicast group address configuration.

When MLD snooping is disabled, all MLD queries are flooded in the ingress VLAN.

When MLD snooping is enabled, received MLD queries are flooded in the ingress VLAN, and a copy of the query is sent to the CPU for processing. From the received query, MLD snooping builds the IPv6 multicast address database. It detects multicast router ports, maintains timers, sets report response time, learns the querier IP source address for the VLAN, learns the querier port in the VLAN, and maintains multicast-address aging.
When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the Catalyst 2960, 2960-S, 2960-C, 2960-X or 2960-CX switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

Note
When a group exists in the MLD snooping database, the switch responds to a group-specific query by sending an MLDv1 report. When the group is unknown, the group-specific query is flooded to the ingress VLAN.

When a host wants to leave a multicast group, it can send out an MLD Done message (equivalent to IGMP Leave message). When the switch receives an MLDv1 Done message, if Immediate-Leave is not enabled, the switch sends an MASQ to the port from which the message was received to determine if other devices connected to the port should remain in the multicast group.

**Multicast Client Aging Robustness**

You can configure port membership removal from addresses based on the number of queries. A port is removed from membership to an address only when there are no reports to the address on the port for the configured number of queries. The default number is 2.

**Multicast Router Discovery**

Like IGMP snooping, MLD snooping performs multicast router discovery, with these characteristics:

- Ports configured by a user never age out.
- Dynamic port learning results from MLDv1 snooping queries and IPv6 PIMv2 packets.
- If there are multiple routers on the same Layer 2 interface, MLD snooping tracks a single multicast router on the port (the router that most recently sent a router control packet).
- Dynamic multicast router port aging is based on a default timer of 5 minutes; the multicast router is deleted from the router port list if no control packet is received on the port for 5 minutes.
- IPv6 multicast router discovery only takes place when MLD snooping is enabled on the switch.
- Received IPv6 multicast router control packets are always flooded to the ingress VLAN, whether or not MLD snooping is enabled on the switch.
- After the discovery of the first IPv6 multicast router port, unknown IPv6 multicast data is forwarded only to the discovered router ports (before that time, all IPv6 multicast data is flooded to the ingress VLAN).

**MLD Reports**

The processing of MLDv1 join messages is essentially the same as with IGMPv2. When no IPv6 multicast routers are detected in a VLAN, reports are not processed or forwarded from the switch. When IPv6 multicast routers are detected and an MLDv1 report is received, an IPv6 multicast group address is entered in the VLAN MLD database. Then all IPv6 multicast traffic to the group within the VLAN is forwarded using this address. When MLD snooping is disabled, reports are flooded in the ingress VLAN.

When MLD snooping is enabled, MLD report suppression, called listener message suppression, is automatically enabled. With report suppression, the switch forwards the first MLDv1 report received by a group to IPv6
multicast routers; subsequent reports for the group are not sent to the routers. When MLD snooping is disabled, report suppression is disabled, and all MLDv1 reports are flooded to the ingress VLAN.

The switch also supports MLDv1 proxy reporting. When an MLDv1 MASQ is received, the switch responds with MLDv1 reports for the address on which the query arrived if the group exists in the switch on another port and if the port on which the query arrived is not the last member port for the address.

MLD Done Messages and Immediate-Leave

When the Immediate-Leave feature is enabled and a host sends an MLDv1 Done message (equivalent to an IGMP leave message), the port on which the Done message was received is immediately deleted from the group. You enable Immediate-Leave on VLANs and (as with IGMP snooping), you should only use the feature on VLANs where a single host is connected to the port. If the port was the last member of a group, the group is also deleted, and the leave information is forwarded to the detected IPv6 multicast routers.

When Immediate Leave is not enabled in a VLAN (which would be the case when there are multiple clients for a group on the same port) and a Done message is received on a port, an MASQ is generated on that port. The user can control when a port membership is removed for an existing address in terms of the number of MASQs. A port is removed from membership to an address when there are no MLDv1 reports to the address on the port for the configured number of queries.

The number of MASQs generated is configured by using the `ipv6 mld snooping last-listener-query count` global configuration command. The default number is 2.

The MASQ is sent to the IPv6 multicast address for which the Done message was sent. If there are no reports sent to the IPv6 multicast address specified in the MASQ during the switch maximum response time, the port on which the MASQ was sent is deleted from the IPv6 multicast address database. The maximum response time is the time configured by using the `ipv6 mld snooping last-listener-query-interval` global configuration command. If the deleted port is the last member of the multicast address, the multicast address is also deleted, and the switch sends the address leave information to all detected multicast routers.

Topology Change Notification Processing

When topology change notification (TCN) solicitation is enabled by using the `ipv6 mld snooping tcn query solicit` global configuration command, MLDv1 snooping sets the VLAN to flood all IPv6 multicast traffic with a configured number of MLDv1 queries before it begins sending multicast data only to selected ports. You set this value by using the `ipv6 mld snooping tcn flood query count` global configuration command. The default is to send two queries. The switch also generates MLDv1 global Done messages with valid link-local IPv6 source addresses when the switch becomes the STP root in the VLAN or when it is configured by the user. This is same as done in IGMP snooping.

How to Configure IPv6 MLD Snooping

Default MLD Snooping Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLD snooping (Global)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>MLD snooping (per VLAN)</td>
<td>Enabled. MLD snooping must be globally enabled for VLAN MLD snooping to take place.</td>
</tr>
<tr>
<td>IPv6 Multicast addresses</td>
<td>None configured.</td>
</tr>
<tr>
<td>IPv6 Multicast router ports</td>
<td>None configured.</td>
</tr>
<tr>
<td>MLD snooping Immediate Leave</td>
<td>Disabled.</td>
</tr>
<tr>
<td>MLD snooping robustness variable</td>
<td>Global: 2; Per VLAN: 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.</td>
</tr>
<tr>
<td>Last listener query count</td>
<td>Global: 2; Per VLAN: 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.</td>
</tr>
<tr>
<td>Last listener query interval</td>
<td>Global: 1000 (1 second); VLAN: 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global interval.</td>
</tr>
<tr>
<td>TCN query solicit</td>
<td>Disabled.</td>
</tr>
<tr>
<td>TCN query count</td>
<td>2.</td>
</tr>
<tr>
<td>MLD listener suppression</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>

### MLD Snooping Configuration Guidelines

When configuring MLD snooping, consider these guidelines:

- You can configure MLD snooping characteristics at any time, but you must globally enable MLD snooping by using the `ipv6 mld snooping` global configuration command for the configuration to take effect.

- When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the switch to receive queries on the VLAN. For normal-range VLANs (1 to 1005), it is not necessary to enable IPv6 MLD snooping on the VLAN on the Catalyst 6500 switch.

- MLD snooping and IGMP snooping act independently of each other. You can enable both features at the same time on the switch.

- The maximum number of address entries allowed for the switch is 1000.
Enabling or Disabling MLD Snooping on the Switch (CLI)

By default, IPv6 MLD snooping is globally disabled on the switch and enabled on all VLANs. When MLD snooping is globally disabled, it is also disabled on all VLANs. When you globally enable MLD snooping, the VLAN configuration overrides the global configuration. That is, MLD snooping is enabled only on VLAN interfaces in the default state (enabled).

You can enable and disable MLD snooping on a per-VLAN basis or for a range of VLANs, but if you globally disable MLD snooping, it is disabled in all VLANs. If global snooping is enabled, you can enable or disable VLAN snooping.

Beginning in privileged EXEC mode, follow these steps to globally enable MLD snooping on the switch:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ipv6 mld snooping</code></td>
<td>Enables MLD snooping on the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)# <code>ipv6 mld snooping</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>reload</code></td>
<td>Reload the operating system.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Switch(config)# <code>reload</code></td>
<td></td>
</tr>
</tbody>
</table>

Enabling or Disabling MLD Snooping on a VLAN (CLI)

Beginning in privileged EXEC mode, follow these steps to enable MLD snooping on a VLAN.
### Configuring a Static Multicast Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure an IPv6 multicast address and member ports for a VLAN.

To add a Layer 2 port as a member of a multicast group, perform this procedure:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Multicast Router Port (CLI)

**Purpose**

Configures a multicast group with a Layer 2 port as a member of a multicast group:

- `vlan-id` is the multicast group VLAN ID. The VLAN ID range is 1 to 1001 and 1006 to 4094.
- `ipv6_multicast_address` is the 128-bit group IPv6 address. The address must be in the form specified in RFC 2373.
- `interface-id` is the member port. It can be a physical interface or a port channel (1 to 6).

**Command or Action**

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>ipv6 mld snooping vlan vlan-id static</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td><code>ipv6_multicast_address interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ipv6 mld snooping vlan 1 static 3333.0000.1111 interface gigabitethernet 0/1</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
</tbody>
</table>

**Step 4**

**Command or Action**

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>end</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>end</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
</tbody>
</table>

**Step 5**

**Command or Action**

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use one of the following:</td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td><code>show ipv6 mld snooping address</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td><code>show ipv6 mld snooping address vlan vlan-id</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td>Switch# <code>show ipv6 mld snooping address</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td>Switch# <code>show ipv6 mld snooping vlan 1</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
</tbody>
</table>

**Note**

Static connections to multicast routers are supported only on switch ports.

Beginning in privileged EXEC mode, follow these steps to add a multicast router port to a VLAN:

**Procedure**

**Command or Action**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
<tr>
<td></td>
<td>Switch# <code>configure terminal</code></td>
<td>Considers the function of a multicast group with Layer 2 port.</td>
</tr>
</tbody>
</table>
IP Multicast Snooping

Enabling MLD Immediate Leave (CLI)

Beginning in privileged EXEC mode, follow these steps to enable MLDv1 Immediate Leave:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure terminal  | Enters global configuration mode. |
| Example:
Switch# configure terminal | |
| **Step 2**
ipv6 mld snooping vlan vlan-id immediate-leave
Example:
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave | Enables MLD Immediate Leave on the VLAN interface. |
| **Step 3**
end
Example:
Switch(config)# end | Returns to privileged EXEC mode. |
| **Step 4**
show ipv6 mld snooping vlan vlan-id
Example:
Switch# show ipv6 mld snooping vlan 1 | Verifies that Immediate Leave is enabled on the VLAN interface. |
## Configuring MLD Snooping Queries (CLI)

Beginning in privileged EXEC mode, follow these steps to configure MLD snooping query characteristics for the switch or for a VLAN:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ipv6 mld snooping robustness-variable value</code></td>
<td>(Optional) Sets the number of queries that are sent before switch will deletes a listener (port) that does not respond to a general query. The range is 1 to 3; the default is 2.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 mld snooping robustness-variable 3</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ipv6 mld snooping vlan vlan-id robustness-variable value</code></td>
<td>(Optional) Sets the robustness variable on a VLAN basis, which determines the number of general queries that MLD snooping sends before aging out a multicast address when there is no MLD report response. The range is 1 to 3; the default is 0. When set to 0, the number used is the global robustness variable value.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 3</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ipv6 mld snooping last-listener-query-count count</code></td>
<td>(Optional) Sets the number of MASQs that the switch sends before aging out an MLD client. The range is 1 to 7; the default is 2. The queries are sent 1 second apart.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 mld snooping last-listener-query-count 7</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ipv6 mld snooping vlan vlan-id last-listener-query-count count</code></td>
<td>(Optional) Sets the last-listener query count on a VLAN basis. This value overrides the value configured globally. The range is 1 to 7; the default is 0. When set to 0, the global count value is used. Queries are sent 1 second apart.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-count 7</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ipv6 mld snooping last-listener-query-interval interval</code></td>
<td>(Optional) Sets the maximum response time that the switch waits after sending out a MASQ before deleting a port from the multicast group. The range is 100 to 32,768 thousands of a second. The default is 1000 (1 second).</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 mld snooping last-listener-query-interval 2000</td>
<td></td>
</tr>
</tbody>
</table>
## Purpose

Command or Action | Purpose |
--- | --- |
**Step 7** | (Optional) Sets the last-listener query interval on a VLAN basis. This value overrides the value configured globally. The range is 0 to 32,768 thousands of a second. The default is 0. When set to 0, the global last-listener query interval is used. |
ipv6 mld snooping vlan *vlan-id*  
last-listener-query-interval *interval* |  |
**Example:**  
Switch(config)# ipv6 mld snooping vlan 1  
last-listener-query-interval 2000 |  |
**Step 8** | (Optional) Enables topology change notification (TCN) solicitation, which means that VLANs flood all IPv6 multicast traffic for the configured number of queries before sending multicast data to only those ports requesting to receive it. The default is for TCN to be disabled. |
ipv6 mld snooping tcn query solicit |  |
**Example:**  
Switch(config)# ipv6 mld snooping tcn query solicit |  |
**Step 9** | (Optional) When TCN is enabled, specifies the number of TCN queries to be sent. The range is from 1 to 10; the default is 2. |
ipv6 mld snooping tcn flood query count *count* |  |
**Example:**  
Switch(config)# ipv6 mld snooping tcn flood query count 5 |  |
**Step 10** | Returns to privileged EXEC mode. |
end |  |
**Step 11** | (Optional) Verifies that the MLD snooping querier information for the switch or for the VLAN. |
show ipv6 mld snooping querier [ vlan *vlan-id*] |  |
**Example:**  
Switch(config)# show ipv6 mld snooping querier  
vlan 1 |  |

## Disabling MLD Listener Message Suppression (CLI)

MLD snooping listener message suppression is enabled by default. When it is enabled, the switch forwards only one MLD report per multicast router query. When message suppression is disabled, multiple MLD reports could be forwarded to the multicast routers.

Beginning in privileged EXEC mode, follow these steps to disable MLD listener message suppression:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
**Step 1** | Enter global configuration mode. |
configure terminal |  |
**Example:**  
Switch# configure terminal |  |
**Step 2** | Disable MLD message suppression. |
no ipv6 mld snooping listener-message-suppression |  |
**Example:**  
Switch(config)# no ipv6 mld snooping listener-message-suppression |  |
### Displaying MLD Snooping Information

You can display MLD snooping information for dynamically learned and statically configured router ports and VLAN interfaces. You can also display IPv6 group address multicast entries for a VLAN configured for MLD snooping.

#### Table 15: Commands for Displaying MLD Snooping Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ipv6 mld snooping</strong> [ vlan vlan-id ]</td>
<td>Displays the MLD snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td><strong>show ipv6 mld snooping mrouter</strong> [ vlan vlan-id ]</td>
<td>Displays information on dynamically learned and manually configured multicast router interfaces. When you enable MLD snooping, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces. (Optional) Enters <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td><strong>show ipv6 mld snooping querier</strong> [ vlan vlan-id ]</td>
<td>Displays information about the IPv6 address and incoming port for the most-recently received MLD query messages in the VLAN. (Optional) Enters <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>
| **show ipv6 mld snooping address** [ count | vlan vlan-id ] | Displays all IPv6 multicast address information or specific IPv6 multicast address information for the switch or a VLAN.  
  - Enters `count` to show the group count on the switch or in a VLAN.  
  - Enters `user` to display MLD snooping user-configured group information for the switch or for a VLAN. |
### Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mld snooping address vlan vlan-id [ipv6-multicast-address]</td>
<td>Displays MLD snooping for the specified VLAN and IPv6 multicast address.</td>
</tr>
</tbody>
</table>

### Configuration Examples for Configuring MLD Snooping

#### Configuring a Static Multicast Group: Example

This example shows how to statically configure an IPv6 multicast group:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static 3333.0000.1111 interface gigabitethernet0/1
Switch(config)# end
```

#### Configuring a Multicast Router Port: Example

This example shows how to add a multicast router port to VLAN 200:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet 0/2
Switch(config)# exit
```

#### Enabling MLD Immediate Leave: Example

This example shows how to enable MLD Immediate Leave on VLAN 130:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

#### Configuring MLD Snooping Queries: Example

This example shows how to set the MLD snooping global robustness variable to 3:

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

This example shows how to set the MLD snooping last-listener query count for a VLAN to 3:

```
Switch# configure terminal
```
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit

This example shows how to set the MLD snooping last-listener query interval (maximum response time) to 2000 (2 seconds):

Switch(config)# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
PART III

IPv6

• Configuring IPv6 ACL, on page 113
CHAPTER 9

Configuring IPv6 ACL

• Finding Feature Information, on page 113
• Information About Configuring IPv6 ACLs, on page 113
• Configuring IPv6 ACLs, on page 114
• Configuration Examples for IPv6 ACL, on page 120

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring IPv6 ACLs

You can filter IP version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP version 4 (IPv4) named ACLs.

Understanding IPv6 ACLs

A switch image supports two types of IPv6 ACLs:

• IPv6 port ACLs - Supported on inbound traffic on Layer 2 interfaces only. Applied to all IPv6 packets entering the interface.

Note

If you configure unsupported IPv6 ACLs, an error message appears and the configuration does not take affect.

The switch does not support VLAN ACLs (VLAN maps) for IPv6 traffic.
You can apply both IPv4 and IPv6 ACLs to an interface.
Supported ACL Features

IPv6 ACLs on the switch have these characteristics:

• Fragmented frames (the fragments keyword as in IPv4) are supported.

• The same statistics supported in IPv4 are supported for IPv6 ACLs.

• If the switch runs out of TCAM space, packets associated with the ACL label are forwarded to the CPU, and the ACLs are applied in software.

IPv6 ACL Limitations

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most Cisco IOS-supported IPv6 ACLs with some exceptions:

• IPv6 source and destination addresses-ACL matching is supported only on prefixes from /0 to /64 and host addresses (/128) that are in the extended universal identifier (EUI)-64 format. The switch supports only these host addresses with no loss of information:
  - aggregatable global unicast addresses
  - link local addresses

• The switch does not support matching on these keywords: flowlabel, routing header, and undetermined-transport.

• The switch does not support reflexive ACLs (the reflect keyword).

• This release supports only port ACLs for IPv6; it does not support router ACLs for IPv6 and VLAN ACLs (VLAN maps).

• The switch does not apply MAC-based ACLs on IPv6 frames.

• You cannot apply IPv6 port ACLs to Layer 2 EtherChannels.

• The switch does not support output port ACLs.

• When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.

• If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

Configuring IPv6 ACLs

To filter IPv6 traffic, you perform these steps:

SUMMARY STEPS

1. Create an IPv6 ACL, and enter IPv6 access list configuration mode.
2. Configure the IPv6 ACL to block (deny) or pass (permit) traffic.
3. Apply the IPv6 ACL to an interface.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Create an IPv6 ACL, and enter IPv6 access list configuration mode.</td>
<td>—</td>
</tr>
<tr>
<td>Step 2 Configure the IPv6 ACL to block (deny) or pass (permit) traffic.</td>
<td>—</td>
</tr>
<tr>
<td>Step 3 Apply the IPv6 ACL to an interface.</td>
<td>—</td>
</tr>
</tbody>
</table>

**Default IPv6 ACL Configuration**

There are no IPv6 ACLs configured or applied.

**Interaction with Other Features and Switches**

- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.
- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the hardware memory is full, for any additional configured ACLs, packets are processed to the CPU, and the ACLs are applied in software. When the hardware is full, a message is printed to the console indicating the ACL has been unloaded and the packets will be processed in software.

**Note**

Only packets of the same type as the ACL that could not be added (ipv4, ipv6, MAC) will be processed in software.

- If the TCAM is full, for any additional configured ACLs, packets are forwarded to the CPU, and the ACLs are applied in software.

**Creating IPv6 ACL**

Follow these steps to create an IPv6 ACL:
### Creating IPv6 ACL

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        | Enters global configuration mode. |
| `configure terminal` | | |
| Example:          | | |
| Switch# `configure terminal` | | |

| **Step 3**        | Define an IPv6 access list name, and enter IPv6 access-list configuration mode. |
| `ipv6access-list` | | |
| `access-list-name` | | |
| Example:          | | |
| `ipv6 access-list access-list-name` | | |

<p>| <strong>Step 4</strong>        | Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions: |
| <code>{deny|permit}</code>    | - For protocol, enter the name or number of an Internet protocol: ahp, esp, icmp, ipv6, pcp, stcp, tcp, or udp, or an integer in the range 0 to 255 representing an IPv6 protocol number. | |
| <code>protocol</code>        | - The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373). | |
| Example:          | - Enter any as an abbreviation for the IPv6 prefix ::/0. | |
| <code>{deny|permit} protocol</code> | - For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons. | |
| Example:          | - (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range. | |
| <code>{deny|permit}=protocol</code> | If the operator follows the source-ipv6-prefix/prefix-length argument, it must match the source port. If the operator follows the destination-ipv6-prefix/ prefix-length argument, it must match the destination port. | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>{deny</td>
<td>permit} tcp</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>{deny</td>
<td>permit} tcp {source-ipv6-prefix/prefix-length</td>
</tr>
<tr>
<td>(Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is ipv6.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter log to cause an logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter routing to specify that IPv6 packets be routed.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><em>syn</em>—Synchronize bit set.</td>
<td></td>
</tr>
<tr>
<td><em>urg</em>—Urgent pointer bit set.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 6

**{deny|permit} udp**

**Example:**
```plaintext
{deny | permit} udp
{source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address}
[operator [port-number]][(destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address)
[operator [port-number]]][dscp value]
[log][log-input]
[neq [port | protocol]] [range [port | protocol]]
[routing][sequence value][time-range name]
```

(Optional) Define a UDP access list and the access conditions.

Enter udp for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the operator [port] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.

### Step 7

**{deny|permit} icmp**

**Example:**
```plaintext
{deny | permit} icmp
{source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address}
[operator [port-number]]
{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address}
[operator [port-number]][icmp-type [icmp-code]
|icmp-message] [dscp value] [log] [log-input]
[routing][sequence value][time-range name]
```

(Optional) Define an ICMP access list and the access conditions.

Enter icmp for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 3a, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

- **icmp-type**—Enter to filter by ICMP message type, a number from 0 to 255.
- **icmp-code**—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.
- **icmp-message**—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the `? key or see command reference for this release.```

### Step 8

**end**

**Example:**
```
Switch(config)# end
```

Returns to privileged EXEC mode.

### Step 9

**show ipv6 access-list**

**Example:**
```
show ipv6 access-list
```

Verify the access list configuration.

### Step 10

**show running-config**

**Example:**
```
```

Verifies your entries.
Applying an IPv6 ACL to an Interface

This section describes how to apply IPv6 ACLs to network interfaces. You can apply an ACL to inbound traffic on Layer 2 interfaces.

Beginning in privileged EXEC mode, follow these steps to control access to an interface:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>interface interface_id</td>
<td>Identify a Layer 2 interface (for port ACLs) on which to apply an access list, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# interface interface-id</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ipv6 traffic-filter access-list-name</td>
<td>Apply the access list to incoming or outgoing traffic on the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# ipv6 traffic-filter access-list-name in</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Verify the access list configuration.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Displaying IPv6 ACLs**

To display IPv6 ACLs, perform this procedure:
### Configuration Examples for IPv6 ACL

#### Example: Creating IPv6 ACL

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic. The second permit entry is necessary because an implicit deny-all condition is at the end of each IPv6 access list.

Note: Logging is supported only on Layer 3 interfaces.

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

#### Example: Displaying IPv6 ACLs

This is an example of the output from the `show access-lists` privileged EXEC command. The output shows all access lists that are configured on the switch.
Switch #show access-lists
Extended IP access list hello
  10 permit ip any any
IPv6 access list ipv6
  permit ipv6 any any sequence 10

This is an example of the output from the show ipv6 access-lists privileged EXEC command. The output shows only IPv6 access lists configured on the switch.

Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30
Example: Displaying IPv6 ACLs
PART IV

Layer 2

- Configuring Spanning Tree Protocol, on page 125
- Configuring Multiple Spanning-Tree Protocol, on page 151
- Configuring Optional Spanning-Tree Features, on page 195
- Configuring EtherChannels, on page 227
- Configuring the MAC Address-Table Move Update Feature, on page 261
- Configuring UniDirectional Link Detection, on page 267
CHAPTER 10

Configuring Spanning Tree Protocol

• Finding Feature Information, on page 125
• Restrictions for STP, on page 125
• Information About Spanning Tree Protocol, on page 126
• How to Configure Spanning-Tree Features, on page 137
• Monitoring Spanning-Tree Status, on page 149

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for STP

• An attempt to configure a switch as the root switch fails if the value necessary to be the root switch is less than 1.

• If your network consists of switches that support and do not support the extended system ID, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

• The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.

• The Catalyst 2960-L switch supports Spanning Tree Protocol for a maximum of 256 VLANs.

• The Catalyst Digital Building Series switch supports Spanning Tree Protocol for a maximum of 24 VLANs.
Information About Spanning Tree Protocol

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Note

By default, the switch sends keepalive messages (to ensure the connection is up) only on interfaces that do not have small form-factor pluggable (SFP) modules. You can change the default for an interface by entering the [no] keepalive interface configuration command with no keywords.
Spanning-Tree Topology and BPDUs

The stable, active spanning-tree topology of a switched network is controlled by these elements:

- The unique bridge ID (switch priority and MAC address) associated with each VLAN on each switch.
- The spanning-tree path cost to the root switch.
- The port identifier (port priority and MAC address) associated with each Layer 2 interface.

When the switches in a network are powered up, each functions as the root switch. Each switch sends a configuration BPDU through all of its ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique bridge ID of the switch that the sending switch identifies as the root switch
- The spanning-tree path cost to the root
- The bridge ID of the sending switch
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a switch receives a configuration BPDU that contains superior information (lower bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the switch, the switch also forwards it with an updated message to all attached LANs for which it is the designated switch.

If a switch receives a configuration BPDU that contains inferior information to that currently stored for that port, it discards the BPDU. If the switch is a designated switch for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

A BPDU exchange results in these actions:

- One switch in the network is elected as the root switch (the logical center of the spanning-tree topology in a switched network). See the figure following the bullets.
  
  For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch. The switch priority value occupies the most significant bits of the bridge ID, as shown in the following figure.

- A root port is selected for each switch (except the root switch). This port provides the best path (lowest cost) when the switch forwards packets to the root switch.

- Only one outgoing port on the stack root switch is selected as the root port. The remaining switches in the stack become its designated switches (Switch 2 and Switch 3) as shown in the following figure.

- The shortest distance to the root switch is calculated for each switch based on the path cost.

- A designated switch for each LAN segment is selected. The designated switch incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.
Figure 4: Spanning-Tree Port States in a Switch Stack

One stack member is elected as the stack root switch. The stack root switch contains the outgoing root port

All paths that are not needed to reach the root switch from anywhere in the switched network are placed in the spanning-tree blocking mode.

Related Topics
  - Configuring the Root Switch, on page 139
  - Restrictions for STP, on page 125

Bridge ID, Device Priority, and Extended System ID

The IEEE 802.1D standard requires that each switch has an unique bridge identifier (bridge ID), which controls the selection of the root switch. Because each VLAN is considered as a different logical bridge with PVST+ and Rapid PVST+, the same switch must have a different bridge ID for each configured VLAN. Each VLAN on the switch has a unique 8-byte bridge ID. The 2 most-significant bytes are used for the switch priority, and the remaining 6 bytes are derived from the switch MAC address.

The switch supports the IEEE 802.1t spanning-tree extensions, and some of the bits previously used for the switch priority are now used as the VLAN identifier. The result is that fewer MAC addresses are reserved for the switch, and a larger range of VLAN IDs can be supported, all while maintaining the uniqueness of the bridge ID.
The 2 bytes previously used for the switch priority are reallocated into a 4-bit priority value and a 12-bit extended system ID value equal to the VLAN ID.

**Table 16: Device Priority Value and Extended System ID**

<table>
<thead>
<tr>
<th>Priority Value</th>
<th>Extended System ID (Set Equal to the VLAN ID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit 16</td>
<td>Bit 15</td>
</tr>
<tr>
<td>32768</td>
<td>16384</td>
</tr>
</tbody>
</table>

Spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN. Because the switch stack appears as a single switch to the rest of the network, all switches in the stack use the same bridge ID for a given spanning tree. If the stack master fails, the stack members recalculate their bridge IDs of all running spanning trees based on the new MAC address of the new stack master.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For example, when you change the switch priority value, you change the probability that the switch will be elected as the root switch. Configuring a higher value decreases the probability; a lower value increases the probability.

If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. 4096 is the value of the least-significant bit of a 4-bit switch priority value as shown in the table.

**Related Topics**
- Configuring the Root Switch, on page 139
- Restrictions for STP, on page 125
- Configuring the Root Switch, on page 172
- Root Switch, on page 154
- Specifying the MST Region Configuration and Enabling MSTP, on page 170

**Port Priority Versus Path Cost**

If a loop occurs, spanning tree uses port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

The spanning-tree path cost default value is derived from the media speed of an interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

**Related Topics**
- Configuring Port Priority, on page 142
- Configuring Path Cost, on page 143
Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When an interface transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each Layer 2 interface on a switch using spanning tree exists in one of these states:

- **Blocking**—The interface does not participate in frame forwarding.
- **Listening**—The first transitional state after the blocking state when the spanning tree decides that the interface should participate in frame forwarding.
- **Learning**—The interface prepares to participate in frame forwarding.
- **Forwarding**—The interface forwards frames.
- **Disabled**—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

An interface moves through these states:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

*Figure 5: Spanning-Tree Interface States*

An interface moves through the states.
When you power up the switch, spanning tree is enabled by default, and every interface in the switch, VLAN, or network goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to move the interface to the blocking state.
2. While spanning tree waits for the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the switch learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

**Blocking State**

A Layer 2 interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to each switch interface. A switch initially functions as the root until it exchanges BPDUs with other switches. This exchange establishes which switch in the network is the root or root switch. If there is only one switch in the network, no exchange occurs, the forward-delay timer expires, and the interface moves to the listening state. An interface always enters the blocking state after switch initialization.

An interface in the blocking state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

**Listening State**

The listening state is the first state a Layer 2 interface enters after the blocking state. The interface enters this state when the spanning tree decides that the interface should participate in frame forwarding.

An interface in the listening state performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

**Learning State**

A Layer 2 interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state.

An interface in the learning state performs these functions:

- Discards frames received on the interface
Forwarding State

A Layer 2 interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs these functions:

- Receives and forwards frames received on the interface
- Forwards frames switched from another interface
- Learns addresses
- Receives BPDUs

Disabled State

A Layer 2 interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational.

A disabled interface performs these functions:

- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Does not receive BPDUs

How a Switch or Port Becomes the Root Switch or Root Port

If all switches in a network are enabled with default spanning-tree settings, the switch with the lowest MAC address becomes the root switch.

Figure 6: Spanning-Tree Topology

Switch A is elected as the root switch because the switch priority of all the switches is set to the default (32768) and Switch A has the lowest MAC address. However, because of traffic patterns, number of forwarding interfaces, or link types, Switch A might not be the ideal root switch. By increasing the priority (lowering the
numerical value) of the ideal switch so that it becomes the root switch, you force a spanning-tree recalculation
to form a new topology with the ideal switch as the root. 

When the spanning-tree topology is calculated based on default parameters, the path between source and
destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links
to an interface that has a higher number than the root port can cause a root-port change. The goal is to make
the fastest link the root port.

For example, assume that one port on Switch B is a Gigabit Ethernet link and that another port on Switch B
(a 10/100 link) is the root port. Network traffic might be more efficient over the Gigabit Ethernet link. By
changing the spanning-tree port priority on the Gigabit Ethernet port to a higher priority (lower numerical
value) than the root port, the Gigabit Ethernet port becomes the new root port.

**Related Topics**

[Configuring Port Priority](#), on page 142

### Spanning Tree and Redundant Connectivity

**Figure 7: Spanning Tree and Redundant Connectivity**

You can create a redundant backbone with spanning tree by connecting two switch interfaces to another device
or to two different devices. Spanning tree automatically disables one interface but enables it if the other one
fails. If one link is high-speed and the other is low-speed, the low-speed link is always disabled. If the speeds
are the same, the port priority and port ID are added together, and spanning tree disables the link with the

highest value.

You can also create redundant links between switches by using EtherChannel groups.
Spanning-Tree Address Management

IEEE 802.1D specifies 17 multicast addresses, ranging from 0x00180C2000000 to 0x0180C2000010, to be used by different bridge protocols. These addresses are static addresses that cannot be removed.

If spanning tree is enabled, the CPU on the switch receives packets destined for 0x0180C2000000 and 0x0180C2000010. If spanning tree is disabled, the switch forwards those packets as unknown multicast addresses.

Accelerated Aging to Retain Connectivity

The default for aging dynamic addresses is 5 minutes, the default setting of the `mac address-table aging-time` global configuration command. However, a spanning-tree reconfiguration can cause many station locations to change. Because these stations could be unreachable for 5 minutes or more during a reconfiguration, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value (`spanning-tree vlan vlan-id forward-time seconds` global configuration command) when the spanning tree reconfigures.

Because each VLAN is a separate spanning-tree instance, the switch accelerates aging on a per-VLAN basis. A spanning-tree reconfiguration on one VLAN can cause the dynamic addresses learned on that VLAN to be subject to accelerated aging. Dynamic addresses on other VLANs can be unaffected and remain subject to the aging interval entered for the switch.

Related Topics
- Configuring the Root Switch, on page 139
- Restrictions for STP, on page 125

Spanning-Tree Modes and Protocols

The switch supports these spanning-tree modes and protocols:

- **PVST⁺**—This spanning-tree mode is based on the IEEE 802.1D standard and Cisco proprietary extensions. The PVST⁺ runs on each VLAN on the switch up to the maximum supported, ensuring that each has a loop-free path through the network.

  The PVST⁺ provides Layer 2 load-balancing for the VLAN on which it runs. You can create different logical topologies by using the VLANs on your network to ensure that all of your links are used but that no one link is oversubscribed. Each instance of PVST⁺ on a VLAN has a single root switch. This root switch propagates the spanning-tree information associated with that VLAN to all other switches in the network. Because each switch has the same information about the network, this process ensures that the network topology is maintained.

- **Rapid PVST⁺**—This spanning-tree mode is the same as PVST⁺ except that is uses a rapid convergence based on the IEEE 802.1w standard. Beginning from 15.2(4)E release, the STP default mode is Rapid PVST⁺. To provide rapid convergence, the Rapid PVST⁺ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST⁺ uses a short aging time for dynamically learned MAC address entries.

  Rapid PVST⁺ uses the same configuration as PVST⁺ (except where noted), and the switch needs only minimal extra configuration. The benefit of Rapid PVST⁺ is that you can migrate a large PVST⁺ install base to Rapid PVST⁺ without having to learn the complexities of the Multiple Spanning Tree Protocol (MSTP) configuration and without having to reprogram your network. In Rapid PVST⁺ mode, each VLAN runs its own spanning-tree instance up to the maximum supported.
• MSTP—This spanning-tree mode is based on the IEEE 802.1s standard. You can map multiple VLANs to the same spanning-tree instance, which reduces the number of spanning-tree instances required to support a large number of VLANs. The MSTP runs on top of the RSTP (based on IEEE 802.1w), which provides for rapid convergence of the spanning tree by eliminating the forward delay and by quickly transitioning root ports and designated ports to the forwarding state.

Related Topics
Changing the Spanning-Tree Mode

Supported Spanning-Tree Instances

In PVST+ or Rapid PVST+ mode, the switch supports up to 64 spanning-tree instances.
In MSTP mode, the switch supports up to 64 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

Related Topics
Disabling Spanning Tree, on page 138
Default Spanning-Tree Configuration, on page 136
Default MSTP Configuration, on page 166

Spanning-Tree Interoperability and Backward Compatibility

In a mixed MSTP and PVST+ network, the common spanning-tree (CST) root must be inside the MST backbone, and a PVST+ switch cannot connect to multiple MST regions.
When a network contains switches running Rapid PVST+ and switches running PVST+, we recommend that the Rapid PVST+ switches and PVST+ switches be configured for different spanning-tree instances. In the Rapid PVST+ spanning-tree instances, the root switch must be a Rapid PVST+ switch. In the PVST+ instances, the root switch must be a PVST+ switch. The PVST+ switches should be at the edge of the network.

Table 17: PVST+, MSTP, and Rapid-PVST+ Interoperability and Compatibility

<table>
<thead>
<tr>
<th></th>
<th>PVST+</th>
<th>MSTP</th>
<th>Rapid PVST+</th>
</tr>
</thead>
<tbody>
<tr>
<td>PVST+</td>
<td>Yes</td>
<td>Yes (with restrictions)</td>
<td>Yes (reverts to PVST+)</td>
</tr>
<tr>
<td>MSTP</td>
<td>Yes (with restrictions)</td>
<td>Yes</td>
<td>Yes (reverts to PVST+)</td>
</tr>
<tr>
<td>Rapid PVST+</td>
<td>Yes (reverts to PVST+)</td>
<td>Yes (reverts to PVST+)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Related Topics
Specifying the MST Region Configuration and Enabling MSTP, on page 170
MSTP Configuration Guidelines, on page 153
Multiple Spanning-Tree Regions, on page 154

STP and IEEE 802.1Q Trunks

The IEEE 802.1Q standard for VLAN trunks imposes some limitations on the spanning-tree strategy for a network. The standard requires only one spanning-tree instance for all VLANs allowed on the trunks. However, in a network of Cisco switches connected through IEEE 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks.
When you connect a Cisco switch to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco switch uses PVST+ to provide spanning-tree interoperability. If Rapid PVST+ is enabled, the switch uses it instead of PVST+. The switch combines the spanning-tree instance of the IEEE 802.1Q VLAN of the trunk with the spanning-tree instance of the non-Cisco IEEE 802.1Q switch.

However, all PVST+ or Rapid PVST+ information is maintained by Cisco switches separated by a cloud of non-Cisco IEEE 802.1Q switches. The non-Cisco IEEE 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.

Rapid PVST+ is automatically enabled on IEEE 802.1Q trunks, and no user configuration is required. The external spanning-tree behavior on access ports is not affected by PVST+.

**VLAN-Bridge Spanning Tree**

Cisco VLAN-bridge spanning tree is used with the fallback bridging feature (bridge groups), which forwards non-IP protocols such as DECnet between two or more VLAN bridge domains or routed ports. The VLAN-bridge spanning tree allows the bridge groups to form a spanning tree on top of the individual VLAN spanning trees to prevent loops from forming if there are multiple connections among VLANs. It also prevents the individual spanning trees from the VLANs being bridged from collapsing into a single spanning tree.

To support VLAN-bridge spanning tree, some of the spanning-tree timers are increased. To use the fallback bridging feature, you must have the IP services feature set enabled on your switch.

### Default Spanning-Tree Configuration

**Table 18: Default Spanning-Tree Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable state</td>
<td>Enabled on VLAN 1.</td>
</tr>
<tr>
<td>Spanning-tree mode</td>
<td>Rapid PVST+ (PVST+ and MSTP are disabled.)</td>
</tr>
<tr>
<td>Switch priority</td>
<td>32768</td>
</tr>
<tr>
<td>Spanning-tree port priority (configurable on a per-interface basis)</td>
<td>128</td>
</tr>
</tbody>
</table>
| Spanning-tree port cost (configurable on a per-interface basis) | 1000 Mb/s: 4  
100 Mb/s: 19  
10 Mb/s: 100  |
| Spanning-tree VLAN port priority (configurable on a per-VLAN basis) | 128                                                   |
| Spanning-tree VLAN port cost (configurable on a per-VLAN basis) | 1000 Mb/s: 4  
100 Mb/s: 19  
10 Mb/s: 100  |
### How to Configure Spanning-Tree Features

#### Changing the Spanning-Tree Mode (CLI)

The switch supports three spanning-tree modes: per-VLAN spanning tree plus (PVST+), Rapid PVST+, or multiple spanning tree protocol (MSTP). By default, the switch runs the Rapid PVST+ protocol.

If you want to enable a mode that is different from the default mode, this procedure is required.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. spanning-tree mode \{pvst | mst | rapid-pvst\}
4. interface interface-id
5. spanning-tree link-type point-to-point
6. end
7. clear spanning-tree detected-protocols

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Configures a spanning-tree mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree mode {pvst</td>
<td>mst</td>
</tr>
<tr>
<td>Example:</td>
<td>• Select pvst to enable PVST+.</td>
</tr>
<tr>
<td></td>
<td>• Select mst to enable MSTP.</td>
</tr>
<tr>
<td></td>
<td>• Select rapid-pvst to enable rapid PVST+.</td>
</tr>
<tr>
<td><strong>Step 4</strong> interface interface-id</td>
<td>Specifies an interface to configure, and enters interface configuration mode. Valid interfaces include physical ports, VLANs, and port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 6.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> spanning-tree link-type point-to-point</td>
<td>Specfies that the link type for this port is point-to-point.</td>
</tr>
<tr>
<td>Example:</td>
<td>If you connect this port (local port) to a remote port through a point-to-point link and the local port becomes a designated port, the switch negotiates with the remote port and rapidly changes the local port to the forwarding state.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> clear spanning-tree detected-protocols</td>
<td>If any port on the switch is connected to a port on a legacy IEEE 802.1D switch, this command restarts the protocol migration process on the entire switch.</td>
</tr>
<tr>
<td>Example:</td>
<td>This step is optional if the designated switch detects that this switch is running rapid PVST+.</td>
</tr>
<tr>
<td>Switch# clear spanning-tree detected-protocols</td>
<td></td>
</tr>
</tbody>
</table>

## Disabling Spanning Tree

Spanning tree is enabled by default on VLAN 1 and on all newly created VLANs up to the spanning-tree limit. Disable spanning tree only if you are sure there are no loops in the network topology.

**Caution**

When spanning tree is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can drastically reduce network performance.

This procedure is optional.

### SUMMARY STEPS

1. enable
2. configure terminal
3. no spanning-tree vlan \textit{vlan-id}
4. end

\textbf{DETAILED STEPS}

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Step 3</strong> no spanning-tree vlan \textit{vlan-id}</td>
</tr>
<tr>
<td>Example:</td>
<td>For \textit{vlan-id}, the range is 1 to 4094.</td>
</tr>
<tr>
<td>Switch(config)# no spanning-tree vlan 300</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

\textbf{Related Topics}

- Supported Spanning-Tree Instances, on page 135
- Default Spanning-Tree Configuration, on page 136

\section*{Configuring the Root Switch}

To configure a switch as the root for the specified VLAN, use the \texttt{spanning-tree vlan vlan-id root} global configuration command to modify the switch priority from the default value (32768) to a significantly lower value. When you enter this command, the software checks the switch priority of the root switches for each VLAN. Because of the extended system ID support, the switch sets its own priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN.

Use the \texttt{diameter} keyword to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the \texttt{hello} keyword to override the automatically calculated hello time.

This procedure is optional.
### SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree vlan *vlan-id* root primary [diameter *net-diameter*]
4. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
*Example:*  
Switch> enable |
| Step 2 | configure terminal | Enters global configuration mode.  
*Example:*  
Switch# configure terminal |
| Step 3 | spanning-tree vlan *vlan-id* root primary [diameter *net-diameter*] | Configures a switch to become the root for the specified VLAN.  
*Example:*  
Switch(config)# spanning-tree vlan 20-24 root primary diameter 4 |
| Step 4 | end | Returns to privileged EXEC mode.  
*Example:*  
Switch(config)# end |

**What to do next**

After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the `spanning-tree vlan *vlan-id* hello-time`, `spanning-tree vlan *vlan-id* forward-time`, and the `spanning-tree vlan *vlan-id* max-age` global configuration commands.

**Related Topics**
- Bridge ID, Device Priority, and Extended System ID, on page 128
- Spanning-Tree Topology and BPDUs, on page 127
- Accelerated Aging to Retain Connectivity, on page 134
Restrictions for STP, on page 125

Configuring a Secondary Root Device

When you configure a switch as the secondary root, the switch priority is modified from the default value (32768) to 28672. With this priority, the switch is likely to become the root switch for the specified VLAN if the primary root switch fails. This is assuming that the other network switches use the default switch priority of 32768, and therefore, are unlikely to become the root switch.

You can execute this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello-time values that you used when you configured the primary root switch with the `spanning-tree vlan vlan-id root primary` global configuration command.

This procedure is optional.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. spanning-tree vlan vlan-id root secondary [diameter net-diameter]
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree vlan vlan-id root secondary [diameter net-diameter]</td>
<td>Configures a switch to become the secondary root for the specified VLAN.</td>
</tr>
<tr>
<td>Example: Switch(config)# spanning-tree vlan 20-24 root secondary diameter 4</td>
<td></td>
</tr>
</tbody>
</table>

- For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

  - (Optional) For `diameter net-diameter`, specify the maximum number of switches between any two end stations. The range is 2 to 7.

  Use the same network diameter value that you used when configuring the primary root switch.
### Configuring Port Priority

If your switch is a member of a switch stack, you must use the `spanning-tree [vlan vlan-id] cost cost` interface configuration command instead of the `spanning-tree [vlan vlan-id] port-priority priority` interface configuration command to select an interface to put in the forwarding state. Assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last.

This procedure is optional.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `spanning-tree port-priority priority`
5. `spanning-tree vlan vlan-id port-priority priority`
6. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
  Example:  
  Switch> enable |
| **Step 2** `configure terminal` | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** `interface interface-id` | Specifies an interface to configure, and enters interface configuration mode.  
  Valid interfaces include physical ports and port-channel logical interfaces (port-channel port-channel-number).  
  Example:  
  Switch(config)# interface gigabitethernet 0/2 |
### Configuring Path Cost

This procedure is optional.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-id
4. spanning-tree cost cost
5. spanning-tree vlan vlan-id cost cost
6. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch# configure terminal</td>
<td>Specifies an interface to configure, and enters interface configuration mode. Valid interfaces include physical ports and port-channel logical interfaces (port-channel port-channel-number).</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;interface interface-id</td>
<td>Configures the cost for an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# interface gigabitethernet 0/1</td>
<td>If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission. For cost, the range is 1 to 200000000; the default value is derived from the media speed of the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;spanning-tree cost cost</td>
<td>Configures the cost for a VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch(config-if)# spanning-tree cost 250</td>
<td>If a loop occurs, spanning tree uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.</td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;spanning-tree vlan vlan-id cost cost</td>
<td>- For vlan-id, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300</td>
<td>- For cost, the range is 1 to 200000000; the default value is derived from the media speed of the interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

The `show spanning-tree interface interface-id` privileged EXEC command displays information only for ports that are in a link-up operative state. Otherwise, you can use the `show running-config` privileged EXEC command to confirm the configuration.

**Related Topics**
- Port Priority Versus Path Cost, on page 129
Configuring the Device Priority of a VLAN

You can configure the switch priority and make it more likely that a standalone switch will be chosen as the root switch.

Exercise care when using this command. For most situations, we recommend that you use the `spanning-tree vlan vlan-id root primary` and the `spanning-tree vlan vlan-id root secondary` global configuration commands to modify the switch priority.

This procedure is optional.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `spanning-tree vlan vlan-id priority priority`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| `enable`         | Enables privileged EXEC mode. |
| Example:          | • Enter your password if prompted. |
| `Switch> enable`  |         |
| **Step 2**
| `configure terminal` | Enters global configuration mode. |
| Example:          |         |
| `Switch# configure terminal` |         |
| **Step 3**
| `spanning-tree vlan vlan-id priority priority` | Configures the switch priority of a VLAN. |
| Example:          | • For `vlan-id`, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| `Switch(config)# spanning-tree vlan 20 priority 8192` | • For `priority`, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch. |
|                   | Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected. |
### Configuring the Hello Time

The hello time is the time interval between configuration messages generated and sent by the root switch. This procedure is optional.

**SUMMARY STEPS**

1. `enable`
2. `spanning-tree vlan vlan-id hello-time seconds`
3. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the hello time of a VLAN. The hello time is the time interval between configuration messages generated and sent by the root switch. These messages mean that the switch is alive.</td>
</tr>
<tr>
<td><code>spanning-tree vlan vlan-id hello-time seconds</code></td>
<td>• For <code>vlan-id</code>, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td><code>Switch(config)# spanning-tree vlan 20-24 hello-time 3</code></td>
<td>• For <code>seconds</code>, the range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Forwarding-Delay Time for a VLAN

This procedure is optional.
SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree vlan vlan-id forward-time seconds
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>spanning-tree vlan vlan-id forward-time seconds</td>
<td>Configures the forward time of a VLAN. The forwarding delay is the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• For vlan-id, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# spanning-tree vlan 20,25 forward-time 18</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For seconds, the range is 4 to 30; the default is 15.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Maximum-Aging Time for a VLAN

This procedure is optional.

SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree vlan vlan-id max-age seconds
4. end
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree vlan vlan-id max-age seconds</td>
<td>Configures the maximum-aging time of a VLAN. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.</td>
</tr>
<tr>
<td>Example: Switch(config)# spanning-tree vlan 20 max-age 30</td>
<td>• For vlan-id, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For seconds, the range is 6 to 40; the default is 20.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Transmit Hold-Count

You can configure the BPDU burst size by changing the transmit hold count value.

**Note**

Changing this parameter to a higher value can have a significant impact on CPU utilization, especially in Rapid PVST+ mode. Lowering this value can slow down convergence in certain scenarios. We recommend that you maintain the default setting.

This procedure is optional.

### Summary Steps

1. enable
2. configure terminal
3. spanning-tree transmit hold-count value
4. end
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable Example: <code>Switch&gt; enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal Example: <code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 spanning-tree transmit hold-count value Example: <code>Switch(config)# spanning-tree transmit hold-count 6</code></td>
<td>Configures the number of BPDUs that can be sent before pausing for 1 second. For value, the range is 1 to 20; the default is 6.</td>
</tr>
<tr>
<td>Step 4 end Example: <code>Switch(config)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Monitoring Spanning-Tree Status

Table 19: Commands for Displaying Spanning-Tree Status

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree active</td>
<td>Displays spanning-tree information on active interfaces only.</td>
</tr>
<tr>
<td>show spanning-tree detail</td>
<td>Displays a detailed summary of interface information.</td>
</tr>
<tr>
<td>show spanning-tree vlan vlan-id</td>
<td>Displays spanning-tree information for the specified VLAN.</td>
</tr>
<tr>
<td>show spanning-tree interface interface-id</td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree interface interface-id portfast</td>
<td>Displays spanning-tree portfast information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree summary [totals]</td>
<td>Displays a summary of interface states or displays the total lines of the STP state section.</td>
</tr>
</tbody>
</table>
To clear spanning-tree counters, use the `clear spanning-tree [interface interface-id]` privileged EXEC command.
CHAPTER 11

Configuring Multiple Spanning-Tree Protocol

• Finding Feature Information, on page 151
• Prerequisites for MSTP, on page 151
• Restrictions for MSTP, on page 152
• Information About MSTP, on page 153
• How to Configure MSTP Features, on page 170
• Examples, on page 188
• Monitoring MST Configuration and Status, on page 192
• Feature Information for MSTP, on page 193

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MSTP

• For two or more switches to be in the same multiple spanning tree (MST) region, they must have the same VLAN-to-instance map, the same configuration revision number, and the same name.

• For load-balancing across redundant paths in the network to work, all VLAN-to-instance mapping assignments must match; otherwise, all traffic flows on a single link.

• For load-balancing between a per-VLAN spanning tree plus (PVST+) and an MST cloud or between a rapid-PVST+ and an MST cloud to work, all MST boundary ports must be forwarding. MST boundary ports are forwarding when the internal spanning tree (IST) master of the MST cloud is the root of the common spanning tree (CST). If the MST cloud consists of multiple MST regions, one of the MST regions must contain the CST root, and all of the other MST regions must have a better path to the root contained within the MST cloud than a path through the PVST+ or rapid-PVST+ cloud. You might have to manually configure the switches in the clouds.
Restrictions for MSTP

- PVST+, Rapid PVST+, and MSTP are supported, but only one version can be active at any time. (For example, all VLANs run PVST+, all VLANs run Rapid PVST+, or all VLANs run MSTP.)

- VLAN Trunking Protocol (VTP) propagation of the MST configuration is not supported. However, you can manually configure the MST configuration (region name, revision number, and VLAN-to-instance mapping) on each switch within the MST region by using the command-line interface (CLI) or through the Simple Network Management Protocol (SNMP) support.

- Partitioning the network into a large number of regions is not recommended. However, if this situation is unavoidable, we recommend that you partition the switched LAN into smaller LANs interconnected by routers or non-Layer 2 devices.

- A region can have one member or multiple members with the same MST configuration; each member must be capable of processing rapid spanning tree protocol (RSTP) Bridge Protocol Data Units (BPDUs). There is no limit to the number of MST regions in a network, but each region can only support up to 65 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

- After configuring a switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the spanning-tree mst hello-time, spanning-tree mst forward-time, and the spanning-tree mst max-age global configuration commands.

### Table 20: PVST+, MSTP, and Rapid PVST+ Interoperability and Compatibility

<table>
<thead>
<tr>
<th></th>
<th>PVST+</th>
<th>MSTP</th>
<th>Rapid PVST+</th>
</tr>
</thead>
<tbody>
<tr>
<td>PVST+</td>
<td>Yes</td>
<td>Yes (with restrictions)</td>
<td>Yes (reverts to PVST+)</td>
</tr>
<tr>
<td>MSTP</td>
<td>Yes (with restrictions)</td>
<td>Yes</td>
<td>Yes (reverts to PVST+)</td>
</tr>
<tr>
<td>Rapid PVST+</td>
<td>Yes (reverts to PVST+)</td>
<td>Yes (reverts to PVST+)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Related Topics

- Specifying the MST Region Configuration and Enabling MSTP, on page 170
- MSTP Configuration Guidelines, on page 153
- Multiple Spanning-Tree Regions, on page 154
- Configuring the Root Switch, on page 172
- Root Switch, on page 154
Information About MSTP

MSTP Configuration

MSTP, which uses RSTP for rapid convergence, enables multiple VLANs to be grouped into and mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs. The MSTP provides for multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs. It improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

Note

The multiple spanning-tree (MST) implementation is based on the IEEE 802.1s standard.

The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network. This deployment provides the highly available network required in a service-provider environment.

When the switch is in the MST mode, the RSTP, which is based on IEEE 802.1w, is automatically enabled. The RSTP provides rapid convergence of the spanning tree through explicit handshaking that eliminates the IEEE 802.1D forwarding delay and quickly transitions root ports and designated ports to the forwarding state.

Both MSTP and RSTP improve the spanning-tree operation and maintain backward compatibility with equipment that is based on the (original) IEEE 802.1D spanning tree, with existing Cisco-proprietary Multiple Instance STP (MISTP), and with existing Cisco PVST+ and rapid per-VLAN spanning-tree plus (Rapid PVST+).

MSTP Configuration Guidelines

- When you enable MST by using the `spanning-tree mode mst` global configuration command, RSTP is automatically enabled.
- For configuration guidelines about UplinkFast, BackboneFast, and cross-stack UplinkFast, see the relevant sections in the Related Topics section.
- When the switch is in MST mode, it uses the long path-cost calculation method (32 bits) to compute the path cost values. With the long path-cost calculation method, the following path cost values are supported:

<table>
<thead>
<tr>
<th>Speed</th>
<th>Path Cost Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mb/s</td>
<td>2,000,000</td>
</tr>
<tr>
<td>100 Mb/s</td>
<td>200,000</td>
</tr>
<tr>
<td>1 Gb/s</td>
<td>20,000</td>
</tr>
<tr>
<td>10 Gb/s</td>
<td>2,000</td>
</tr>
<tr>
<td>100 Gb/s</td>
<td>200</td>
</tr>
</tbody>
</table>
Root Switch

The switch maintains a spanning-tree instance for the group of VLANs mapped to it. A switch ID, consisting of the switch priority and the switch MAC address, is associated with each instance. For a group of VLANs, the switch with the lowest switch ID becomes the root switch.

When you configure a switch as the root, you modify the switch priority from the default value (32768) to a significantly lower value so that the switch becomes the root switch for the specified spanning-tree instance. When you enter this command, the switch checks the switch priorities of the root switches. Because of the extended system ID support, the switch sets its own priority for the specified instance to 24576 if this value will cause this switches to become the root for the specified spanning-tree instance.

If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value. For more information, select "Bridge ID, Switch Priority, and Extended System ID" link in Related Topics.

If your network consists of switches that support and do not support the extended system ID, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches running older software.

The root switch for each spanning-tree instance should be a backbone or distribution switch. Do not configure an access switch as the spanning-tree primary root.

Use the **diameter** keyword, which is available only for MST instance 0, to specify the Layer 2 network diameter (that is, the maximum number of switch hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically sets an optimal hello time, forward-delay time, and maximum-age time for a network of that diameter, which can significantly reduce the convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

Related Topics

- Configuring the Root Switch, on page 172
- Restrictions for MSTP, on page 152
- Bridge ID, Device Priority, and Extended System ID, on page 128

Multiple Spanning-Tree Regions

For switches to participate in multiple spanning-tree (MST) instances, you must consistently configure the switches with the same MST configuration information. A collection of interconnected switches that have the same MST configuration comprises an MST region.
The MST configuration controls to which MST region each switch belongs. The configuration includes the name of the region, the revision number, and the MST VLAN-to-instance assignment map. You configure the switch for a region by specifying the MST region configuration on it. You can map VLANs to an MST instance, specify the region name, and set the revision number. For instructions and an example, select the "Specifying the MST Region Configuration and Enabling MSTP" link in Related Topics.

A region can have one or multiple members with the same MST configuration. Each member must be capable of processing RSTP bridge protocol data units (BPDUs). There is no limit to the number of MST regions in a network, but each region can support up to 65 spanning-tree instances. Instances can be identified by any number in the range from 0 to 4094. You can assign a VLAN to only one spanning-tree instance at a time.

Related Topics
- Illustration of MST Regions, on page 157
- Specifying the MST Region Configuration and Enabling MSTP, on page 170
- Prerequisites for MSTP, on page 151
- Restrictions for MSTP, on page 152
- Spanning-Tree Interoperability and Backward Compatibility, on page 135
- Optional Spanning-Tree Configuration Guidelines
- BackboneFast, on page 199
- UplinkFast, on page 197

**IST, CIST, and CST**

Unlike PVST+ and Rapid PVST+ in which all the spanning-tree instances are independent, the MSTP establishes and maintains two types of spanning trees:

- An internal spanning tree (IST), which is the spanning tree that runs in an MST region.

  Within each MST region, the MSTP maintains multiple spanning-tree instances. Instance 0 is a special instance for a region, known as the internal spanning tree (IST). All other MST instances are numbered from 1 to 4094.

  The IST is the only spanning-tree instance that sends and receives BPDUs. All of the other spanning-tree instance information is contained in M-records, which are encapsulated within MSTP BPDUs. Because the MSTP BPDU carries information for all instances, the number of BPDUs that need to be processed to support multiple spanning-tree instances is significantly reduced.

  All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth. By default, all VLANs are assigned to the IST.

  An MST instance is local to the region; for example, MST instance 1 in region A is independent of MST instance 1 in region B, even if regions A and B are interconnected.

- A common and internal spanning tree (CIST), which is a collection of the ISTs in each MST region, and the common spanning tree (CST) that interconnects the MST regions and single spanning trees.

  The spanning tree computed in a region appears as a subtree in the CST that encompasses the entire switched domain. The CIST is formed by the spanning-tree algorithm running among switches that support the IEEE 802.1w, IEEE 802.1s, and IEEE 802.1D standards. The CIST inside an MST region is the same as the CST outside a region.
Operations Within an MST Region

The IST connects all the MSTP switches in a region. When the IST converges, the root of the IST becomes the CIST regional root (called the IST master before the implementation of the IEEE 802.1s standard). It is the switch within the region with the lowest switch ID and path cost to the CIST root. The CIST regional root is also the CIST root if there is only one region in the network. If the CIST root is outside the region, one of the MSTP switches at the boundary of the region is selected as the CIST regional root.

When an MSTP switch initializes, it sends BPDUs claiming itself as the root of the CIST and the CIST regional root, with both of the path costs to the CIST root and to the CIST regional root set to zero. The switch also initializes all of its MST instances and claims to be the root for all of them. If the switch receives superior MST root information (lower switch ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the CIST regional root.

During initialization, a region might have many subregions, each with its own CIST regional root. As switches receive superior IST information, they leave their old subregions and join the new subregion that contains the true CIST regional root. All subregions shrink except for the one that contains the true CIST regional root.

For correct operation, all switches in the MST region must agree on the same CIST regional root. Therefore, any two switches in the region only synchronize their port roles for an MST instance if they converge to a common CIST regional root.

Related Topics
Illustration of MST Regions, on page 157

Operations Between MST Regions

If there are multiple regions or legacy IEEE 802.1D switches within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP switches in the network. The MST instances combine with the IST at the boundary of the region to become the CST.

The IST connects all the MSTP switches in the region and appears as a subtree in the CIST that encompasses the entire switched domain. The root of the subtree is the CIST regional root. The MST region appears as a virtual switch to adjacent STP switches and MST regions.

Only the CST instance sends and receives BPDUs, and MST instances add their spanning-tree information into the BPDUs to interact with neighboring switches and compute the final spanning-tree topology. Because of this, the spanning-tree parameters related to BPDU transmission (for example, hello time, forward time, max-age, and max-hops) are configured only on the CST instance but affect all MST instances. Parameters related to the spanning-tree topology (for example, switch priority, port VLAN cost, and port VLAN priority) can be configured on both the CST instance and the MST instance.

MSTP switches use Version 3 RSTP BPDUs or IEEE 802.1D STP BPDUs to communicate with legacy IEEE 802.1D switches. MSTP switches use MSTP BPDUs to communicate with MSTP switches.

Related Topics
Illustration of MST Regions, on page 157

IEEE 802.1s Terminology

Some MST naming conventions used in Cisco’s prestandard implementation have been changed to identify some internal or regional parameters. These parameters are significant only within an MST region, as opposed to external parameters that are relevant to the whole network. Because the CIST is the only spanning-tree instance that spans the whole network, only the CIST parameters require the external rather than the internal or regional qualifiers.
The CIST root is the root switch for the unique instance that spans the whole network, the CIST.

The CIST external root path cost is the cost to the CIST root. This cost is left unchanged within an MST region. Remember that an MST region looks like a single switch for the CIST. The CIST external root path cost is the root path cost calculated between these virtual switches and switches that do not belong to any region.

The CIST regional root was called the IST master in the prestandard implementation. If the CIST root is in the region, the CIST regional root is the CIST root. Otherwise, the CIST regional root is the closest switch to the CIST root in the region. The CIST regional root acts as a root switch for the IST.

The CIST internal root path cost is the cost to the CIST regional root in a region. This cost is only relevant to the IST, instance 0.

Table 21: Prestandard and Standard Terminology

<table>
<thead>
<tr>
<th>IEEE Standard</th>
<th>Cisco Prestandard</th>
<th>Cisco Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIST regional root</td>
<td>IST master</td>
<td>CIST regional root</td>
</tr>
<tr>
<td>CIST internal root path cost</td>
<td>IST master path cost</td>
<td>CIST internal path cost</td>
</tr>
<tr>
<td>CIST external root path cost</td>
<td>Root path cost</td>
<td>Root path cost</td>
</tr>
<tr>
<td>MSTI regional root</td>
<td>Instance root</td>
<td>Instance root</td>
</tr>
<tr>
<td>MSTI internal root path cost</td>
<td>Root path cost</td>
<td>Root path cost</td>
</tr>
</tbody>
</table>

Illustration of MST Regions

This figure displays three MST regions and a legacy IEEE 802.1D switch (D). The CIST regional root for region 1 (A) is also the CIST root. The CIST regional root for region 2 (B) and the CIST regional root for region 3 (C) are the roots for their respective subtrees within the CIST. The RSTP runs in all regions.
Hop Count

The IST and MST instances do not use the message-age and maximum-age information in the configuration BPDU to compute the spanning-tree topology. Instead, they use the path cost to the root and a hop-count mechanism similar to the IP time-to-live (TTL) mechanism.

By using the `spanning-tree mst max-hops` global configuration command, you can configure the maximum hops inside the region and apply it to the IST and all MST instances in that region. The hop count achieves the same result as the message-age information (triggers a reconfiguration). The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDU it generates. When the count reaches zero, the switch discards the BPDU and ages the information held for the port.

The message-age and maximum-age information in the RSTP portion of the BPDU remain the same throughout the region, and the same values are propagated by the region designated ports at the boundary.
Boundary Ports

In the Cisco prestandard implementation, a boundary port connects an MST region to a single spanning-tree region running RSTP, to a single spanning-tree region running PVST+ or rapid PVST+, or to another MST region with a different MST configuration. A boundary port also connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

There is no definition of a boundary port in the IEEE 802.1s standard. The IEEE 802.1Q-2002 standard identifies two kinds of messages that a port can receive:

- internal (coming from the same region)
- external (coming from another region)

When a message is internal, the CIST part is received by the CIST, and each MST instance receives its respective M-record.

When a message is external, it is received only by the CIST. If the CIST role is root or alternate, or if the external BPDU is a topology change, it could have an impact on the MST instances.

An MST region includes both switches and LANs. A segment belongs to the region of its designated port. Therefore, a port in a different region than the designated port for a segment is a boundary port. This definition allows two ports internal to a region to share a segment with a port belonging to a different region, creating the possibility of a port receiving both internal and external messages.

The primary change from the Cisco prestandard implementation is that a designated port is not defined as boundary, unless it is running in an STP-compatible mode.

**Note**

If there is a legacy STP switch on the segment, messages are always considered external.

The other change from the Cisco prestandard implementation is that the CIST regional root switch ID field is now inserted where an RSTP or legacy IEEE 802.1Q switch has the sender switch ID. The whole region performs like a single virtual switch by sending a consistent sender switch ID to neighboring switches. In this example, switch C would receive a BPDU with the same consistent sender switch ID of root, whether or not A or B is designated for the segment.

IEEE 802.1s Implementation

The Cisco implementation of the IEEE MST standard includes features required to meet the standard, as well as some of the desirable prestandard functionality that is not yet incorporated into the published standard.

Port Role Naming Change

The boundary role is no longer in the final MST standard, but this boundary concept is maintained in Cisco’s implementation. However, an MST instance port at a boundary of the region might not follow the state of the corresponding CIST port. Two boundary roles currently exist:

- The boundary port is the root port of the CIST regional root—When the CIST instance port is proposed and is in sync, it can send back an agreement and move to the forwarding state only after all the corresponding MSTI ports are in sync (and thus forwarding). The MSTI ports now have a special *master* role.
• The boundary port is not the root port of the CIST regional root—The MSTI ports follow the state and role of the CIST port. The standard provides less information, and it might be difficult to understand why an MSTI port can be alternately blocking when it receives no BPDUs (MRecords). In this case, although the boundary role no longer exists, the show commands identify a port as boundary in the type column of the output.

Interoperation Between Legacy and Standard Switches

Because automatic detection of prestandard switches can fail, you can use an interface configuration command to identify prestandard ports. A region cannot be formed between a standard and a prestandard switch, but they can interoperate by using the CIST. Only the capability of load-balancing over different instances is lost in that particular case. The CLI displays different flags depending on the port configuration when a port receives prestandard BPDUs. A syslog message also appears the first time a switch receives a prestandard BPDU on a port that has not been configured for prestandard BPDU transmission.

Figure 9: Standard and Prestandard Switch Interoperation

Assume that A is a standard switch and B a prestandard switch, both configured to be in the same region. A is the root switch for the CIST, and B has a root port (BX) on segment X and an alternate port (BY) on segment Y. If segment Y flaps, and the port on BY becomes the alternate before sending out a single prestandard BPDU, AY cannot detect that a prestandard switch is connected to Y and continues to send standard BPDUs. The port BY is fixed in a boundary, and no load balancing is possible between A and B. The same problem exists on segment X, but B might transmit topology

Note

We recommend that you minimize the interaction between standard and prestandard MST implementations.

Detecting Unidirectional Link Failure

This feature is not yet present in the IEEE MST standard, but it is included in this Cisco IOS release. The software checks the consistency of the port role and state in the received BPDUs to detect unidirectional link failures that could cause bridging loops.

When a designated port detects a conflict, it keeps its role, but reverts to the discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.
This figure illustrates a unidirectional link failure that typically creates a bridging loop. Switch A is the root switch, and its BPDUs are lost on the link leading to switch B. RSTP and MST BPDU include the role and state of the sending port. With this information, switch A can detect that switch B does not react to the superior BPDUs it sends and that switch B is the designated, not root switch. As a result, switch A blocks (or keeps blocking) its port, which prevents the bridging loop.

**Interoperability with IEEE 802.1D STP**

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy IEEE 802.1D switches. If this switch receives a legacy IEEE 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only IEEE 802.1D BPDU on that port. An MSTP switch also can detect that a port is at the boundary of a region when it receives a legacy BPDU, an MSTP BPDU (Version 3) associated with a different region, or an RSTP BPDU (Version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives IEEE 802.1D BPDU because it cannot detect whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. A switch might also continue to assign a boundary role to a port when the switch to which this switch is connected has joined the region. To restart the protocol migration process (force the renegotiation with neighboring switches), use the `clear spanning-tree detected-protocols` privileged EXEC command.

If all the legacy switches on the link are RSTP switches, they can process MSTP BPDU as if they are RSTP BPDU. Therefore, MSTP switches send either a Version 0 configuration and TCN BPDU or Version 3 MSTP BPDU on a boundary port. A boundary port connects to a LAN, the designated switch of which is either a single spanning-tree switch or a switch with a different MST configuration.

**RSTP Overview**

The RSTP takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second (in contrast to 50 seconds with the default settings in the IEEE 802.1D spanning tree).

**Port Roles and the Active Topology**

The RSTP provides rapid convergence of the spanning tree by assigning port roles and by learning the active topology. The RSTP builds upon the IEEE 802.1D STP to select the switch with the highest switch priority (lowest numerical priority value) as the root switch. The RSTP then assigns one of these port roles to individual ports:

- Root port—Provides the best path (lowest cost) when the switch forwards packets to the root switch.
- Designated port—Connects to the designated switch, which incurs the lowest path cost when forwarding packets from that LAN to the root switch. The port through which the designated switch is attached to the LAN is called the designated port.
• Alternate port—Offers an alternate path toward the root switch to that provided by the current root port.

• Backup port—Acts as a backup for the path provided by a designated port toward the leaves of the spanning tree. A backup port can exist only when two ports are connected in a loopback by a point-to-point link or when a switch has two or more connections to a shared LAN segment.

• Disabled port—Has no role within the operation of the spanning tree.

A port with the root or a designated port role is included in the active topology. A port with the alternate or backup port role is excluded from the active topology.

In a stable topology with consistent port roles throughout the network, the RSTP ensures that every root port and designated port immediately transition to the forwarding state while all alternate and backup ports are always in the discarding state (equivalent to blocking in IEEE 802.1D). The port state controls the operation of the forwarding and learning processes.

<table>
<thead>
<tr>
<th>Operational Status</th>
<th>STP Port State (IEEE 802.1D)</th>
<th>RSTP Port State</th>
<th>Is Port Included in the Active Topology?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Blocking</td>
<td>Discarding</td>
<td>No</td>
</tr>
<tr>
<td>Enabled</td>
<td>Listening</td>
<td>Discarding</td>
<td>No</td>
</tr>
<tr>
<td>Enabled</td>
<td>Learning</td>
<td>Learning</td>
<td>Yes</td>
</tr>
<tr>
<td>Enabled</td>
<td>Forwarding</td>
<td>Forwarding</td>
<td>Yes</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>Discarding</td>
<td>No</td>
</tr>
</tbody>
</table>

To be consistent with Cisco STP implementations, this guide defines the port state as *blocking* instead of *discarding*. Designated ports start in the listening state.

### Rapid Convergence

The RSTP provides for rapid recovery of connectivity following the failure of a switch, a switch port, or a LAN. It provides rapid convergence for edge ports, new root ports, and ports connected through point-to-point links as follows:

• Edge ports—If you configure a port as an edge port on an RSTP switch by using the `spanning-tree portfast` interface configuration command, the edge port immediately transitions to the forwarding state. An edge port is the same as a Port Fast-enabled port, and you should enable it only on ports that connect to a single end station.

• Root ports—If the RSTP selects a new root port, it blocks the old root port and immediately transitions the new root port to the forwarding state.

• Point-to-point links—If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

![Proposal and Agreement Handshaking for Rapid Convergence](image-url)
Switch A sends a proposal message (a configuration BPDU with the proposal flag set) to Switch B, proposing itself as the designated switch.

After receiving the proposal message, Switch B selects as its new root port the port from which the proposal message was received, forces all nonedge ports to the blocking state, and sends an agreement message (a BPDU with the agreement flag set) through its new root port.

After receiving Switch B’s agreement message, Switch A also immediately transitions its designated port to the forwarding state. No loops in the network are formed because Switch B blocked all of its nonedge ports and because there is a point-to-point link between Switches A and B.

When Switch C is connected to Switch B, a similar set of handshaking messages are exchanged. Switch C selects the port connected to Switch B as its root port, and both ends immediately transition to the forwarding state. With each iteration of this handshaking process, one more switch joins the active topology. As the network converges, this proposal-agreement handshaking progresses from the root toward the leaves of the spanning tree.

The switch learns the link type from the port duplex mode: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection. You can override the default setting that is controlled by the duplex setting by using the `spanning-tree link-type` interface configuration command.

![Diagram of RSTP handshaking](image-url)

**Synchronization of Port Roles**

When the switch receives a proposal message on one of its ports and that port is selected as the new root port, the RSTP forces all other ports to synchronize with the new root information.

The switch is synchronized with superior root information received on the root port if all other ports are synchronized. An individual port on the switch is synchronized if

- That port is in the blocking state.
- It is an edge port (a port configured to be at the edge of the network).
If a designated port is in the forwarding state and is not configured as an edge port, it transitions to the blocking state when the RSTP forces it to synchronize with new root information. In general, when the RSTP forces a port to synchronize with root information and the port does not satisfy any of the above conditions, its port state is set to blocking.

**Figure 12: Sequence of Events During Rapid Convergence**

After ensuring that all of the ports are synchronized, the switch sends an agreement message to the designated switch corresponding to its root port. When the switches connected by a point-to-point link are in agreement about their port roles, the RSTP immediately transitions the port states to forwarding.

### Bridge Protocol Data Unit Format and Processing

The RSTP BPDU format is the same as the IEEE 802.1D BPDU format except that the protocol version is set to 2. A new 1-byte Version 1 Length field is set to zero, which means that no version 1 protocol information is present.

#### Table 23: RSTP BPDU Flags

<table>
<thead>
<tr>
<th>Bit</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Topology change (TC)</td>
</tr>
<tr>
<td>1</td>
<td>Proposal</td>
</tr>
<tr>
<td>2–3</td>
<td>Port role:</td>
</tr>
<tr>
<td>00</td>
<td>Unknown</td>
</tr>
<tr>
<td>01</td>
<td>Alternate port</td>
</tr>
<tr>
<td>10</td>
<td>Root port</td>
</tr>
<tr>
<td>11</td>
<td>Designated port</td>
</tr>
<tr>
<td>4</td>
<td>Learning</td>
</tr>
<tr>
<td>Bit</td>
<td>Function</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>Forwarding</td>
</tr>
<tr>
<td>6</td>
<td>Agreement</td>
</tr>
<tr>
<td>7</td>
<td>Topology change acknowledgement (TCA)</td>
</tr>
</tbody>
</table>

The sending switch sets the proposal flag in the RSTP BPDU to propose itself as the designated switch on that LAN. The port role in the proposal message is always set to the designated port.

The sending switch sets the agreement flag in the RSTP BPDU to accept the previous proposal. The port role in the agreement message is always set to the root port.

The RSTP does not have a separate topology change notification (TCN) BPDU. It uses the topology change (TC) flag to show the topology changes. However, for interoperability with IEEE 802.1D switches, the RSTP switch processes and generates TCN BPDDUs.

The learning and forwarding flags are set according to the state of the sending port.

### Processing Superior BPDU Information

If a port receives superior root information (lower switch ID, lower path cost, and so forth) than currently stored for the port, the RSTP triggers a reconfiguration. If the port is proposed and is selected as the new root port, RSTP forces all the other ports to synchronize.

If the BPDU received is an RSTP BPDU with the proposal flag set, the switch sends an agreement message after all of the other ports are synchronized. If the BPDU is an IEEE 802.1D BPDU, the switch does not set the proposal flag and starts the forward-delay timer for the port. The new root port requires twice the forward-delay time to transition to the forwarding state.

If the superior information received on the port causes the port to become a backup or alternate port, RSTP sets the port to the blocking state but does not send the agreement message. The designated port continues sending BPDDUs with the proposal flag set until the forward-delay timer expires, at which time the port transitions to the forwarding state.

### Processing Inferior BPDU Information

If a designated port receives an inferior BPDU (such as a higher switch ID or a higher path cost than currently stored for the port) with a designated port role, it immediately replies with its own information.

### Topology Changes

This section describes the differences between the RSTP and the IEEE 802.1D in handling spanning-tree topology changes.

- **Detection**—Unlike IEEE 802.1D in which any transition between the blocking and the forwarding state causes a topology change, only transitions from the blocking to the forwarding state cause a topology change with RSTP (only an increase in connectivity is considered a topology change). State changes on an edge port do not cause a topology change. When an RSTP switch detects a topology change, it deletes the learned information on all of its non-edge ports except on those from which it received the TC notification.

- **Notification**—Unlike IEEE 802.1D, which uses TCN BPDDUs, the RSTP does not use them. However, for IEEE 802.1D interoperability, an RSTP switch processes and generates TCN BPDDUs.
- Acknowledgement—When an RSTP switch receives a TCN message on a designated port from an IEEE 802.1D switch, it replies with an IEEE 802.1D configuration BPDU with the TCA bit set. However, if the TC-while timer (the same as the topology-change timer in IEEE 802.1D) is active on a root port connected to an IEEE 802.1D switch and a configuration BPDU with the TCA bit set is received, the TC-while timer is reset.

This behavior is only required to support IEEE 802.1D switches. The RSTP BPDUs never have the TCA bit set.

- Propagation—When an RSTP switch receives a TC message from another switch through a designated or root port, it propagates the change to all of its nonedge, designated ports and to the root port (excluding the port on which it is received). The switch starts the TC-while timer for all such ports and flushes the information learned on them.

- Protocol migration—For backward compatibility with IEEE 802.1D switches, RSTP selectively sends IEEE 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.

When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which RSTP BPDUs are sent), and RSTP BPDUs are sent. While this timer is active, the switch processes all BPDUs received on that port and ignores the protocol type.

If the switch receives an IEEE 802.1D BPDU after the port migration-delay timer has expired, it assumes that it is connected to an IEEE 802.1D switch and starts using only IEEE 802.1D BPDUs. However, if the RSTP switch is using IEEE 802.1D BPDUs on a port and receives an RSTP BPDU after the timer has expired, it restarts the timer and starts using RSTP BPDUs on that port.

### Protocol Migration Process

A switch running MSTP supports a built-in protocol migration mechanism that enables it to interoperate with legacy IEEE 802.1D switches. If this switch receives a legacy IEEE 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only IEEE 802.1D BPDUs on that port. An MSTP switch also can detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or an RST BPDU (Version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot detect whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. A switch also might continue to assign a boundary role to a port when the switch to which it is connected has joined the region.

### Related Topics
- [Restarting the Protocol Migration Process](#) , on page 185

### Default MSTP Configuration

**Table 24: Default MSTP Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning-tree mode</td>
<td>MSTP</td>
</tr>
<tr>
<td>Switch priority (configurable on a per-CIST port basis)</td>
<td>32768</td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
### About MST-to-PVST+ Interoperability (PVST+ Simulation)

The PVST+ simulation feature enables seamless interoperability between MST and Rapid PVST+. You can enable or disable this per port, or globally. PVST+ simulation is enabled by default.

However, you may want to control the connection between MST and Rapid PVST+ to protect against accidentally connecting an MST-enabled port to a Rapid PVST+-enabled port. Because Rapid PVST+ is the default STP mode, you may encounter many Rapid PVST+-enabled connections.

Disabling this feature causes the switch to stop the MST region from interacting with PVST+ regions. The MST-enabled port moves to a PVST peer inconsistent (blocking) state once it detects it is connected to a Rapid PVST+-enabled port. This port remains in the inconsistent state until the port stops receiving Shared Spanning Tree Protocol (SSTP) BPDUs, and then the port resumes the normal STP transition process.

You can for instance, disable PVST+ simulation, to prevent an incorrectly configured switch from connecting to a network where the STP mode is not MSTP (the default mode is PVST+).

Observe these guidelines when you configure MST switches (in the same region) to interact with PVST+ switches:

- Configure the root for all VLANs inside the MST region as shown in this example:

```bash
Switch# show spanning-tree mst interface gigabitethernet 1/1
GigabitEthernet1/1 of MST00 is root forwarding
Edge port: no  (trunk) port guard : none (default)
Link type: point-to-point (auto) bpdu filter: disable (default)
Boundary : boundary (PVST) bpdu guard : disable (default)
Bpdus sent 10, received 310
```
The ports that belong to the MST switch at the boundary simulate PVST+ and send PVST+ BPDUs for all the VLANs.

If you enable loop guard on the PVST+ switches, the ports might change to a loop-inconsistent state when the MST switches change their configuration. To correct the loop-inconsistent state, you must disable and re-enable loop guard on that PVST+ switch.

- Do not locate the root for some or all of the VLANs inside the PVST+ side of the MST switch because when the MST switch at the boundary receives PVST+ BPDUs for all or some of the VLANs on its designated ports, root guard sets the port to the blocking state.

- When you connect a PVST+ switch to two different MST regions, the topology change from the PVST+ switch does not pass beyond the first MST region. In such a case, the topology changes are propagated only in the instance to which the VLAN is mapped. The topology change stays local to the first MST region, and the Cisco Access Manager (CAM) entries in the other region are not flushed. To make the topology change visible throughout other MST regions, you can map that VLAN to IST or connect the PVST+ switch to the two regions through access links.

- When you disable the PVST+ simulation, note that the PVST+ peer inconsistency can also occur while the port is already in other states of inconsistency. For example, the root bridge for all STP instances must all be in either the MST region or the Rapid PVST+ side. If the root bridge for all STP instances are not on one side or the other, the software moves the port into a PVST+ simulation-inconsistent state.

Note

We recommend that you put the root bridge for all STP instances in the MST region.

About Detecting Unidirectional Link Failure

The dispute mechanism that detects unidirectional link failures is included in the IEEE 802.1D-2004 RSTP and IEEE 802.1Q-2005 MSTP standard, and requires no user configuration.

The switch checks the consistency of the port role and state in the BPDUs it receives, to detect unidirectional link failures that could cause bridging loops. When a designated port detects a conflict, it keeps its role, but reverts to a discarding (blocking) state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.

For example, in the figure below, Switch A is the root bridge and Switch B is the designated port. BPDUs from Switch A are lost on the link leading to switch B.

Figure 13: Detecting Unidirectional Link Failure
Since Rapid PVST+ (802.1w) and MST BPDUs include the role and state of the sending port, Switch A detects (from the inferior BPDU), that switch B does not react to the superior BPDUs it sends, because switch B has the role of a designated port and not the root bridge. As a result, switch A blocks (or keeps blocking) its port, thus preventing the bridging loop.

Note these guidelines and limitations relating to the dispute mechanism:

- It works only on switches running RSTP or MST (the dispute mechanism requires reading the role and state of the port initiating BPDUs).
- It may result in loss of connectivity. For example, in the figure below, Bridge A cannot transmit on the port it elected as a root port. As a result of this situation, there is loss of connectivity (r1 and r2 are designated, a1 is root and a2 is alternate. There is only a one way connectivity between A and R).

**Figure 14: Loss of Connectivity**

- It may cause permanent bridging loops on shared segments. For example, in the figure below, suppose that bridge R has the best priority, and that port b1 cannot receive any traffic from the shared segment 1 and sends inferior designated information on segment 1. Both r1 and a1 can detect this inconsistency. However, with the current dispute mechanism, only r1 will revert to discarding while the root port a1 opens a permanent loop. However, this problem does not occur in Layer 2 switched networks that are connected by point-to-point links.

**Figure 15: Bridging Loops on Shared Segments**
How to Configure MSTP Features

Specifying the MST Region Configuration and Enabling MSTP

For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can only support up to 65 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree mst configuration
4. instance instance-id vlan vlan-range
5. name name
6. revision version
7. show pending
8. exit
9. spanning-tree mode mst
10. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>spanning-tree mst configuration</td>
<td>Enters MST configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# spanning-tree mst configuration</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>instance instance-id vlan vlan-range</td>
<td>Maps VLANs to an MST instance.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-mst)# instance 1 vlan 10-20</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- For `instance-id`, the range is 0 to 4094.
- For `vlan vlan-range`, the range is 1 to 4094.

When you map VLANs to an MST instance, the mapping is incremental, and the VLANs specified in the command are added to or removed from the VLANs that were previously mapped.

To specify a VLAN range, use a hyphen; for example, `instance 1 vlan 1-63` maps VLANs 1 through 63 to MST instance 1.

To specify a VLAN series, use a comma; for example, `instance 1 vlan 10, 20, 30` maps VLANs 10, 20, and 30 to MST instance 1.

**Step 5**

<table>
<thead>
<tr>
<th>name name</th>
<th>Specifies the configuration name. The <code>name</code> string has a maximum length of 32 characters and is case sensitive.</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config-mst)# name region1
```

**Step 6**

<table>
<thead>
<tr>
<th>revision version</th>
<th>Specifies the configuration revision number. The range is 0 to 65535.</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config-mst)# revision 1
```

**Step 7**

<table>
<thead>
<tr>
<th>show pending</th>
<th>Verifies your configuration by displaying the pending configuration.</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config-mst)# show pending
```

**Step 8**

<table>
<thead>
<tr>
<th>exit</th>
<th>Applies all changes, and returns to global configuration mode.</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config-mst)# exit
```

**Step 9**

<table>
<thead>
<tr>
<th>spanning-tree mode mst</th>
<th>Enables MSTP. RSTP is also enabled.</th>
</tr>
</thead>
</table>

Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

You cannot run both MSTP and PVST+ or both MSTP and Rapid PVST+ at the same time.

**Example:**

```
Switch(config)# spanning-tree mode mst
```

**Step 10**

<table>
<thead>
<tr>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config)# end
```
Configuring the Root Switch

This procedure is optional.

Before you begin

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

You must also know the specified MST instance ID. Step 2 in the example uses 0 as the instance ID because that was the instance ID set up by the instructions listed under Related Topics.

SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree mst instance-id root primary
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Configures a switch as the root switch.</td>
</tr>
<tr>
<td>Example:</td>
<td>• For <code>instance-id</code>, you can specify a single instance, a range of</td>
</tr>
<tr>
<td></td>
<td>instances separated by a hyphen, or a series of instances separated</td>
</tr>
<tr>
<td></td>
<td>by a comma. The range is 0 to 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# spanning-tree mst</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instance-id root primary</td>
</tr>
<tr>
<td>Step 4</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- [Root Switch](#), on page 154
- [Specifying the MST Region Configuration and Enabling MSTP](#), on page 170
- [Restrictions for MSTP](#), on page 152
- [Bridge ID, Device Priority, and Extended System ID](#), on page 128
- [Configuring a Secondary Root Switch](#), on page 173

**Configuring a Secondary Root Switch**

When you configure a switch with the extended system ID support as the secondary root, the switch priority is modified from the default value (32768) to 28672. The switch is then likely to become the root switch for the specified instance if the primary root switch fails. This is assuming that the other network switches use the default switch priority of 32768 and therefore are unlikely to become the root switch.

You can execute this command on more than one switch to configure multiple backup root switches. Use the same network diameter and hello-time values that you used when you configured the primary root switch with the `spanning-tree mst instance-id root primary` global configuration command.

This procedure is optional.

**Before you begin**

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.
You must also know the specified MST instance ID. This example uses 0 as the instance ID because that was the instance ID set up by the instructions listed under Related Topics.

**SUMMARY STEPS**

1. **`enable`**
2. **`configure terminal`**
3. **`spanning-tree mst instance-id root secondary`**
4. **`end`**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>spanning-tree mst instance-id root secondary</code></td>
<td>Configures a switch as the secondary root switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# spanning-tree mst 0 root secondary</code></td>
<td>• For <code>instance-id</code>, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Specifying the MST Region Configuration and Enabling MSTP, on page 170
- Configuring the Root Switch, on page 172

**Configuring Port Priority**

If a loop occurs, the MSTP uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
This procedure is optional.

Before you begin
A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

You must also know the specified MST instance ID and the interface used. This example uses 0 as the instance ID and GigabitEthernet0/1 as the interface because that was the instance ID and interface set up by the instructions listed under Related Topics.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. spanning-tree mst instance-id port-priority priority
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies an interface to configure, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> spanning-tree mst instance-id port-priority priority</td>
<td>Configures port priority.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# spanning-tree mst 0 port-priority 64</td>
<td>• For instance-id, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For priority, the range is 0 to 240 in increments of 16. The default is 128. The lower the number, the higher the priority.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>The priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected.</td>
<td></td>
</tr>
</tbody>
</table>

Step 5  
end  
Example:  
Switch(config-if)# end  
Returns to privileged EXEC mode.

The `show spanning-tree mst interface interface-id` privileged EXEC command displays information only if the port is in a link-up operative state. Otherwise, you can use the `show running-config interface` privileged EXEC command to confirm the configuration.

Related Topics  
Specifying the MST Region Configuration and Enabling MSTP, on page 170  
Configuring Path Cost, on page 176

### Configuring Path Cost

The MSTP path cost default value is derived from the media speed of an interface. If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

This procedure is optional.

**Before you begin**

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

You must also know the specified MST instance ID and the interface used. This example uses 0 as the instance ID and GigabitEthernet0/1 as the interface because that was the instance ID and interface set up by the instructions listed under Related Topics.

**SUMMARY STEPS**

1. `enable`  
2. `configure terminal`  
3. `interface interface-id`  
4. `spanning-tree mst instance-id cost cost`  
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Step 2**  
configure terminal  
**Example:**  
Switch# configure terminal  

Enters global configuration mode.

**Step 3**  
interface interface-id  
**Example:**  
Switch(config)# interface gigabitethernet 0/1  

Specifies an interface to configure, and enters interface configuration mode. Valid interfaces include physical ports and port-channel logical interfaces. The port-channel range is 1 to 48.

**Step 4**  
spanning-tree mst instance-id cost cost  
**Example:**  
Switch(config-if)# spanning-tree mst 0 cost 17031970  

Configures the cost.  
If a loop occurs, the MSTP uses the path cost when selecting an interface to place into the forwarding state. A lower path cost represents higher-speed transmission.  
• For *instance-id*, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.  
• For *cost*, the range is 1 to 200000000; the default value is derived from the media speed of the interface.

**Step 5**  
end  
**Example:**  
Switch(config-if)# end  

Returns to privileged EXEC mode.

The *show spanning-tree mst interface interface-id* privileged EXEC command displays information only for ports that are in a link-up operative state. Otherwise, you can use the *show running-config* privileged EXEC command to confirm the configuration.

**Related Topics**  
Configuring Port Priority , on page 174  
Specifying the MST Region Configuration and Enabling MSTP , on page 170

**Configuring the Switch Priority**

Changing the priority of a switch makes it more likely to be chosen as the root switch whether it is a standalone switch.
Exercise care when using this command. For normal network configurations, we recommend that you use the `spanning-tree mst instance-id root primary` and the `spanning-tree mst instance-id root secondary` global configuration commands to specify a switch as the root or secondary root switch. You should modify the switch priority only in circumstances where these commands do not work.

This procedure is optional.

**Before you begin**

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

You must also know the specified MST instance ID used. This example uses 0 as the instance ID because that was the instance ID set up by the instructions listed under Related Topics.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. `spanning-tree mst instance-id priority priority`
4. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>spanning-tree mst instance-id priority priority</code></td>
<td>Configures the switch priority.</td>
</tr>
<tr>
<td>Example:</td>
<td>• For <em>instance-id</em>, you can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.</td>
</tr>
<tr>
<td>Switch(config)# <code>spanning-tree mst 0 priority 40960</code></td>
<td>• For <em>priority</em>, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch.</td>
</tr>
</tbody>
</table>
Configuring the Hello Time

The hello time is the time interval between configuration messages generated and sent by the root switch. This procedure is optional.

Before you begin
A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. spanning-tree mst hello-time seconds  
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1.   | enable            | Enables privileged EXEC mode.  
  | Example:          | • Enter your password if prompted. |
  | Switch> enable    |         |
| 2.   | configure terminal| Enters global configuration mode. |
  | Example:          |         |
  | Switch# configure terminal |   |
Configuring the Forwarding-Delay Time

Before you begin

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree mst forward-time seconds
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree mst forward-time seconds</td>
<td>Configures the forward time for all MST instances. The forwarding delay is the number of seconds a port waits</td>
</tr>
</tbody>
</table>
### Configuring the Maximum-Aging Time

**Before you begin**

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `spanning-tree mst max-age seconds`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the maximum-aging time for all MST instances. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.</td>
</tr>
<tr>
<td><code>spanning-tree mst max-age seconds</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# spanning-tree mst max-age 40</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Maximum-Hop Count

This procedure is optional.

#### Before you begin

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree mst max-hops `hop-count`
4. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree mst max-hops <code>hop-count</code></td>
<td>Specifies the number of hops in a region before the BPDUs is discarded, and the information held for a port is aged. For <code>hop-count</code>, the range is 1 to 255; the default is 20.</td>
</tr>
<tr>
<td>Example: Switch(config)# spanning-tree mst max-hops 25</td>
<td></td>
</tr>
</tbody>
</table>
Specifying the Link Type to Ensure Rapid Transitions

If you connect a port to another port through a point-to-point link and the local port becomes a designated port, the RSTP negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

By default, the link type is controlled from the duplex mode of the interface: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection. If you have a half-duplex link physically connected point-to-point to a single port on a remote switch running MSTP, you can override the default setting of the link type and enable rapid transitions to the forwarding state.

This procedure is optional.

Before you begin

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

You must also know the specified MST instance ID and the interface used. This example uses 0 as the instance ID and GigabitEthernet0/1 as the interface because that was the instance ID and interface set up by the instructions listed under Related Topics.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `spanning-tree link-type point-to-point`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
</tbody>
</table>

Enters global configuration mode.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>interface interface-id</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
</tr>
</tbody>
</table>

Specifies an interface to configure, and enters interface configuration mode. Valid interfaces include physical ports, VLANs, and port-channel logical interfaces. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>spanning-tree link-type point-to-point</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# spanning-tree link-type point-to-point</td>
</tr>
</tbody>
</table>

Specifies that the link type of a port is point-to-point.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# end</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.

**Related Topics**

*Specifying the MST Region Configuration and Enabling MST*, on page 170

### Designating the Neighbor Type

A topology could contain both prestandard and IEEE 802.1s standard compliant devices. By default, ports can automatically detect prestandard devices, but they can still receive both standard and prestandard BPDUs. When there is a mismatch between a device and its neighbor, only the CIST runs on the interface.

You can choose to set a port to send only prestandard BPDUs. The prestandard flag appears in all the `show` commands, even if the port is in STP compatibility mode.

This procedure is optional.

**Before you begin**

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-id
4. spanning-tree mst pre-standard
5. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  * enable
    * Example: Switch> enable
  | Enables privileged EXEC mode.
  * Enter your password if prompted. |
| **Step 2**
  * configure terminal
    * Example: Switch# configure terminal
  | Enters global configuration mode. |
| **Step 3**
  * interface interface-id
    * Example: Switch(config)# interface gigabitethernet 0/1
  | Specifies an interface to configure, and enters interface configuration mode. Valid interfaces include physical ports. |
| **Step 4**
  * spanning-tree mst pre-standard
    * Example: Switch(config-if)# spanning-tree mst pre-standard
  | Specifies that the port can send only prestandard BPDUs. |
| **Step 5**
  * end
    * Example: Switch(config-if)# end
  | Returns to privileged EXEC mode. |

### Related Topics
Specifying the MST Region Configuration and Enabling MSTP, on page 170

### Restarting the Protocol Migration Process

This procedure restarts the protocol migration process and forces renegotiation with neighboring switches. It reverts the switch to MST mode. It is needed when the switch no longer receives IEEE 802.1D BPDUs after it has been receiving them.

Follow these steps to restart the protocol migration process (force the renegotiation with neighboring switches) on the switch.

**Before you begin**

A multiple spanning tree (MST) must be specified and enabled on the switch. For instructions, see Related Topics.

If you want to use the interface version of the command, you must also know the MST interface used. This example uses GigabitEthernet0/1 as the interface because that was the interface set up by the instructions listed under Related Topics.
SUMMARY STEPS

1. enable
2. Enter one of the following commands:
   - clear spanning-tree detected-protocols
   - clear spanning-tree detected-protocols interface interface-id

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter one of the following commands:</td>
</tr>
<tr>
<td></td>
<td>- clear spanning-tree detected-protocols</td>
</tr>
<tr>
<td></td>
<td>- clear spanning-tree detected-protocols interface interface-id</td>
</tr>
<tr>
<td>Example: Switch# clear spanning-tree detected-protocols or Switch# clear spanning-tree detected-protocols interface gigabitethernet 0/1</td>
<td></td>
</tr>
</tbody>
</table>

What to do next

This procedure may need to be repeated if the switch receives more legacy IEEE 802.1D configuration BPDUs (BPDUs with the protocol version set to 0).

Related Topics

- Specifying the MST Region Configuration and Enabling MSTP, on page 170
- Protocol Migration Process, on page 166

Configuring PVST+ Simulation

PVST+ simulation is enabled by default. This means that all ports automatically interoperate with a connected device that is running in Rapid PVST+ mode. If you disabled the feature and want to re-configure it, refer to the following tasks.

To enable PVST+ simulation globally, perform this task:

SUMMARY STEPS

1. enable
2. configure terminal
3. spanning-tree mst simulate pvst global
4. **end**

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
enable  
Example: Switch> enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2**  
configure terminal  
Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 3**  
spanning-tree mst simulate pvst global  
Example: Switch(config)# spanning-tree mst simulate pvst global | Enables PVST+ simulation globally.  
To prevent the switch from automatically interoperating with a connecting switch that is running Rapid PVST+, enter the **no** version of the command. |
| **Step 4**  
end  
Example: Switch(config)# end | Returns to privileged EXEC mode. |

## Enabling PVST+ Simulation on a Port

To enable PVST+ simulation on a port, perform this task:

### SUMMARY STEPS

1. enable  
2. configure terminal  
3. interface interface-id  
4. spanning-tree mst simulate pvst  
5. end  
6. show spanning-tree summary

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
enable  
Example: | Enables privileged EXEC mode.  
• Enter your password if prompted. |
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Selects a port to configure.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gi1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> spanning-tree mst simulate pvst</td>
<td>Enables PVST+ simulation on the specified interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>To prevent a specified interface from automatically interoperating with a connecting switch that is not running MST, enter the <code>spanning-tree mst simulate pvst disable</code> command.</td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree mst simulate pvst</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show spanning-tree summary</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show spanning-tree summary</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

#### Examples: PVST+ Simulation

This example shows how to prevent the switch from automatically interoperating with a connecting switch that is running Rapid PVST+:

```
Switch# configure terminal
Switch(config)# no spanning-tree mst simulate pvst global
```

This example shows how to prevent a port from automatically interoperating with a connecting device that is running Rapid PVST+:

```
Switch(config)# interface1/0/10
Switch(config-if)# spanning-tree mst simulate pvst disable
```
The following sample output shows the system message you receive when a SSTP BPDU is received on a port and PVST+ simulation is disabled:

Message
SPANTREE_PVST_PEER_BLOCK: PVST BPDU detected on port %s [port number].

Severity
Critical

Explanation
A PVST+ peer was detected on the specified interface on the switch. PVST+ simulation feature is disabled, as a result of which the interface was moved to the spanning tree Blocking state.

Action
Identify the PVST+ switch from the network which might be configured incorrectly.

The following sample output shows the system message you receive when peer inconsistency on the interface is cleared:

Message
SPANTREE_PVST_PEER_UNBLOCK: Unblocking port %s [port number].

Severity
Critical

Explanation
The interface specified in the error message has been restored to normal spanning tree state.

Action
None.

This example shows the spanning tree status when port 1/0/10/1 has been configured to disable PVST+ simulation and is currently in the peer type inconsistent state:

Switch# show spanning-tree
VLAN0010
Spanning tree enabled protocol mstp
Root ID Priority 32778
  Address 0002.172c.f400
  This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
  Address 0002.172c.f400
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- -------------------------
Gi1/0/10/1 Desg BKN*4 128.270 P2p *PVST_Peer_Inc

This example shows the spanning tree summary when PVST+ simulation is enabled in the MSTP mode:
Switch# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
PVST Simulation Default is enabled

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST0</td>
<td></td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 mst</td>
<td></td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

This example shows the spanning tree summary when PVST+ simulation is disabled in any STP mode:

Switch# show spanning-tree summary
Switch is in mst mode (IEEE Standard)
Root bridge for: MST0
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
PVST Simulation Default is enabled

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>MST0</td>
<td></td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 mst</td>
<td></td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

This example shows the spanning tree summary when the switch is not in MSTP mode, that is, the switch is in PVST or Rapid-PVST mode. The output string displays the current STP mode:

Switch# show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001, VLAN2001-VLAN2002
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
PVST Simulation Default is enabled but inactive in rapid-pvst mode

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>VLAN2001</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>VLAN2002</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

3 vlans 6 0 0 0 6

This example shows the interface details when PVST+ simulation is globally enabled, or the default configuration:

```
Switch# show spanning-tree interface1/0/10/1 detail
Port 269 (GigabitEthernet1/0/10/1) of VLAN0002 is forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.297.
  Designated root has priority 32769, address 0013.5f20.01c0
  Designated bridge has priority 32769, address 0013.5f20.01c0
  Designated port id is 128.297, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  PVST Simulation is enabled by default
  BPDU: sent 132, received 1
```

This example shows the interface details when PVST+ simulation is globally disabled:

```
Switch# show spanning-tree interface1/0/10/1 detail
Port 269 (GigabitEthernet1/0/10/1) of VLAN0002 is forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.297.
  Designated root has priority 32769, address 0013.5f20.01c0
  Designated bridge has priority 32769, address 0013.5f20.01c0
  Designated port id is 128.297, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  PVST Simulation is disabled by default
  BPDU: sent 132, received 1
```

This example shows the interface details when PVST+ simulation is explicitly enabled on the port:

```
Switch# show spanning-tree interface1/0/10/1 detail
Port 269 (GigabitEthernet1/0/10/1) of VLAN0002 is forwarding
  Port path cost 4, Port priority 128, Port Identifier 128.297.
  Designated root has priority 32769, address 0013.5f20.01c0
  Designated bridge has priority 32769, address 0013.5f20.01c0
  Designated port id is 128.297, designated path cost 0
  Timers: message age 0, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default
  PVST Simulation is enabled
  BPDU: sent 132, received 1
```

This example shows the interface details when the PVST+ simulation feature is disabled and a PVST Peer inconsistency has been detected on the port:

```
Switch# show spanning-tree interface1/0/10/1 detail
```
Port 269 (GigabitEthernet1/0/10/1) of VLAN0002 is broken (PVST Peer Inconsistent)
Port path cost 4, Port priority 128, Port Identifier 128.297.
Designated root has priority 32769, address 0013.5f20.01c0
Designated bridge has priority 32769, address 0013.5f20.01c0
Designated port id is 128.297, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
PVST Simulation is disabled
BPDU: sent 132, received 1

Examples: Detecting Unidirectional Link Failure

This example shows the spanning tree status when port 1/0/10/1 detail has been configured to disable PVST+ simulation and the port is currently in the peer type inconsistent state:

Switch# show spanning-tree
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID Priority 32778
  Address 0002.172c.f400
  This bridge is the root
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
  Address 0002.172c.f400
  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
  Aging Time 300

  Interface Role Sts Cost Prio.Nbr Type
  ---------------- ---- --- --------- -------- -------------------------
  Gi1/0/10/1 Desg BKN 4 128.270  P2p Dispute

This example shows the interface details when a dispute condition is detected:

Switch# show spanning-tree interface1/0/10/1 detail
Port 269 (GigabitEthernet1/0/10/1) of VLAN0002 is designated blocking (dispute)
Port path cost 4, Port priority 128, Port Identifier 128.297.
Designated root has priority 32769, address 0013.5f20.01c0
Designated bridge has priority 32769, address 0013.5f20.01c0
Designated port id is 128.297, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 132, received 1

Monitoring MST Configuration and Status

Table 25: Commands for Displaying MST Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show spanning-tree mst configuration</code></td>
<td>Displays the MST region configuration.</td>
</tr>
<tr>
<td><code>show spanning-tree mst configuration digest</code></td>
<td>Displays the MD5 digest included in the current MSTCI.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>show spanning-tree mst</code></td>
<td>Displays MST information for the all instances. <strong>Note</strong> This command displays information for ports in a link-up operative state.</td>
</tr>
<tr>
<td><code>show spanning-tree mst instance-id</code></td>
<td>Displays MST information for the specified instance. <strong>Note</strong> This command displays information only if the port is in a link-up operative state.</td>
</tr>
<tr>
<td><code>show spanning-tree mst interface interface-id</code></td>
<td>Displays MST information for the specified interface.</td>
</tr>
</tbody>
</table>

**Feature Information for MSTP**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
</tbody>
</table>
Feature Information for MSTP
Configuring Optional Spanning-Tree Features

- Finding Feature Information, on page 195
- Restriction for Optional Spanning-Tree Features, on page 195
- Information About Optional Spanning-Tree Features, on page 196
- How to Configure Optional Spanning-Tree Features, on page 206
- Examples, on page 222
- Monitoring the Spanning-Tree Status, on page 225
- Feature Information for Optional Spanning-Tree Features, on page 225

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restriction for Optional Spanning-Tree Features

- PortFast minimizes the time that interfaces must wait for spanning tree to converge, so it is effective only when used on interfaces connected to end stations. If you enable PortFast on an interface connecting to another switch, you risk creating a spanning-tree loop.

Related Topics
- Enabling PortFast, on page 206
- PortFast, on page 196
Information About Optional Spanning-Tree Features

PortFast

PortFast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states.

*Figure 16: PortFast-Enabled Interfaces*

You can use PortFast on interfaces connected to a single workstation or server to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge. Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An interface with PortFast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

You can enable this feature by enabling it on either the interface or on all nontrunking ports.

**Related Topics**

- *Enabling PortFast*, on page 206
- *Restriction for Optional Spanning-Tree Features*, on page 195

BPDU Guard

The Bridge Protocol Data Unit (BPDU) guard feature can be globally enabled on the switch or can be enabled per port, but the feature operates with some differences.

When you enable BPDU guard at the global level on PortFast edge-enabled ports, spanning tree shuts down ports that are in a PortFast edge-operational state if any BPDU is received on them. In a valid configuration, PortFast edge-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast edge-enabled port means an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. When this happens, the switch shuts down the entire port on which the violation occurred.

When you enable BPDU guard at the interface level on any port without also enabling the PortFast edge feature, and the port receives a BPDU, it is put in the error-disabled state.
The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

Related Topics
   Enabling BPDU Guard, on page 208

BPDU Filtering

The BPDU filtering feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

Enabling BPDU filtering on PortFast edge-enabled interfaces at the global level keeps those interfaces that are in a PortFast edge-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a PortFast edge-enabled interface, the interface loses its PortFast edge-operational status, and BPDU filtering is disabled.

Enabling BPDU filtering on an interface without also enabling the PortFast edge feature keeps the interface from sending or receiving BPDUs.

Caution

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can enable the BPDU filtering feature for the entire switch or for an interface.

Related Topics
   Enabling BPDU Filtering, on page 209

UplinkFast

Figure 17: Switches in a Hierarchical Network

Switches in hierarchical networks can be grouped into backbone switches, distribution switches, and access switches. This complex network has distribution switches and access switches that each have at least one
redundant link that spanning tree blocks to prevent

If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. You can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself by enabling UplinkFast. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures.

When the spanning tree reconfigures the new root port, other interfaces flood the network with multicast packets, one for each address that was learned on the interface. You can limit these bursts of multicast traffic by reducing the max-update-rate parameter (the default for this parameter is 150 packets per second). However, if you enter zero, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

**Note**

UplinkFast is most useful in wiring-closet switches at the access or edge of the network. It is not appropriate for backbone devices. This feature might not be useful for other types of applications.

UplinkFast provides fast convergence after a direct link failure and achieves load-balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 interfaces (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.
Figure 18: UplinkFast Example Before Direct Link Failure

This topology has no link failures. Switch A, the root switch, is connected directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 interface on Switch C that is connected directly to Switch B is in a blocking state.

Figure 19: UplinkFast Example After Direct Link Failure

If Switch C detects a link failure on the currently active link L2 on the root port (a direct link failure), UplinkFast unblocks the blocked interface on Switch C and transitions it to the forwarding state without going through the listening and learning states. This change takes approximately 1 to 5 seconds.

Related Topics
Specifying the MST Region Configuration and Enabling MSTP, on page 170
MSTP Configuration Guidelines, on page 153
Multiple Spanning-Tree Regions, on page 154
Enabling UplinkFast for Use with Redundant Links, on page 210
Events That Cause Fast Convergence

BackboneFast

BackboneFast detects indirect failures in the core of the backbone. BackboneFast is a complementary technology to the UplinkFast feature, which responds to failures on links directly connected to access switches. BackboneFast optimizes the maximum-age timer, which controls the amount of time the switch stores protocol information received on an interface. When a switch receives an inferior BPDU from the designated port of another switch, the BPDU is a signal that the other switch might have lost its path to the root, and BackboneFast tries to find an alternate path to the root.

BackboneFast starts when a root port or blocked interface on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the
designated switch. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an indirect link) has failed (that is, the designated switch has lost its connection to the root switch). Under spanning-tree rules, the switch ignores inferior BPDU for the maximum aging time (default is 20 seconds).

The switch tries to find if it has an alternate path to the root switch. If the inferior BPDU arrives on a blocked interface, the root port and other blocked interfaces on the switch become alternate paths to the root switch. (Self-looped ports are not considered alternate paths to the root switch.) If the inferior BPDU arrives on the root port, all blocked interfaces become alternate paths to the root switch. If the inferior BPDU arrives on the root port and there are no blocked interfaces, the switch assumes that it has lost connectivity to the root switch, causes the maximum aging time on the root port to expire, and becomes the root switch according to normal spanning-tree rules.

If the switch discovers that it still has an alternate path to the root, it expires the maximum aging time on the interface that received the inferior BPDU. If all the alternate paths to the root switch indicate that the switch has lost connectivity to the root switch, the switch expires the maximum aging time on the interface that received the RLQ reply. If one or more alternate paths can still connect to the root switch, the switch makes all interfaces on which it received an inferior BPDU its designated ports and moves them from the blocking state (if they were in the blocking state), through the listening and learning states, and into the forwarding state.

*Figure 20: BackboneFast Example Before Indirect Link Failure*

This is an example topology with no link failures. Switch A, the root switch, connects directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 interface on Switch C that connects directly to Switch B is in the blocking state.

*Figure 21: BackboneFast Example After Indirect Link Failure*

If link L1 fails, Switch C cannot detect this failure because it is not connected directly to link L1. However, because Switch B is directly connected to the root switch over L1, it detects the failure, elects itself the root, and begins sending BPDU to Switch C, identifying itself as the root. When Switch C receives the inferior BPDU from Switch B, Switch C assumes that an indirect failure has occurred. At that point, BackboneFast allows the blocked interface on Switch C to move immediately to the listening state without waiting for the maximum aging time for the interface to expire. BackboneFast then transitions the Layer 2 interface on Switch C to the forwarding state, providing a path from Switch B to Switch A. The root-switch election takes approximately 30 seconds, twice the Forward Delay time if the default Forward Delay time of 15 seconds is
set. BackboneFast reconfigures the topology to account for the failure of link L1.

![Figure 22: Adding a Switch in a Shared-Medium Topology](image)

If a new switch is introduced into a shared-medium topology, BackboneFast is not activated because the inferior BPDUs did not come from the recognized designated switch (Switch B). The new switch begins sending inferior BPDUs that indicate it is the root switch. However, the other switches ignore these inferior BPDUs, and the new switch learns that Switch B is the designated switch to Switch A, the root switch.

**Related Topics**
- Specifying the MST Region Configuration and Enabling MSTP, on page 170
- MSTP Configuration Guidelines, on page 153
- Multiple Spanning-Tree Regions, on page 154
- Enabling BackboneFast, on page 213

**EtherChannel Guard**

You can use EtherChannel guard to detect an EtherChannel misconfiguration between the switch and a connected device. A misconfiguration can occur if the switch interfaces are configured in an EtherChannel, but the interfaces on the other device are not. A misconfiguration can also occur if the channel parameters are not the same at both ends of the EtherChannel.
If the switch detects a misconfiguration on the other device, EtherChannel guard places the switch interfaces in the error-disabled state, and displays an error message.

**Related Topics**

[Enabling EtherChannel Guard](#), on page 214

---

**Root Guard**

**Figure 23: Root Guard in a Service-Provider Network**

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch. You can avoid this situation by enabling root guard on SP switch interfaces that connect to switches in your customer’s network. If spanning-tree calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface in the root-inconsistent (blocked) state to prevent the customer’s switch from becoming the root switch or being in the path to the root.

If a switch outside the SP network becomes the root switch, the interface is blocked (root-inconsistent state), and spanning tree selects a new root switch. The customer’s switch does not become the root switch and is not in the path to the root.

If the switch is operating in multiple spanning-tree (MST) mode, root guard forces the interface to be a designated port. If a boundary port is blocked in an internal spanning-tree (IST) instance because of root guard, the interface also is blocked in all MST instances. A boundary port is an interface that connects to a LAN, the designated switch of which is either an IEEE 802.1D switch or a switch with a different MST region configuration.

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. VLANs can be grouped and mapped to an MST instance.

---

**Caution**

Misuse of the root guard feature can cause a loss of connectivity.
Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is enabled on the entire switched network. Loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if the interface is blocked by loop guard in all MST instances. On a boundary port, loop guard blocks the interface in all MST instances.

Related Topics
Enabling Loop Guard, on page 216

STP PortFast Port Types

You can configure a spanning tree port as an edge port, a network port, or a normal port. A port can be in only one of these states at a given time. The default spanning tree port type is normal. You can configure the port type either globally or per interface.

Depending on the type of device to which the interface is connected, you can configure a spanning tree port as one of these port types:

• A PortFast edge port—is connected to a Layer 2 host. This can be either an access port or an edge trunk port (portfast edge trunk). This type of port interface immediately transitions to the forwarding state, bypassing the listening and learning states. Use PortFast edge on Layer 2 access ports connected to a single workstation or server to allow those devices to connect to the network immediately, rather than waiting for spanning tree to converge.

Even if the interface receives a bridge protocol data unit (BPDU), spanning tree does not place the port into the blocking state. Spanning tree sets the port’s operating state to non-port fast even if the configured state remains port fast edge and starts participating in the topology change.

Note
If you configure a port connected to a Layer 2 switch or bridge as an edge port, you might create a bridging loop.

• A PortFast network port—is connected only to a Layer 2 switch or bridge. Bridge Assurance is enabled only on PortFast network ports. For more information, refer to Bridge Assurance.

Note
If you configure a port that is connected to a Layer 2 host as a spanning tree network port, the port will automatically move into the blocking state.

• A PortFast normal port—is the default type of spanning tree port.
Beginning with Cisco IOS Release 15.2(4)E, or IOS XE 3.8.0E, if you enter the spanning-tree portfast [trunk] command in the global or interface configuration mode, the system automatically saves it as spanning-tree portfast edge [trunk].

Related Topics

Enabling PortFast Port Types, on page 217

Bridge Assurance

You can use Bridge Assurance to help prevent looping conditions that are caused by unidirectional links (one-way traffic on a link or port), or a malfunction in a neighboring switch. Here a malfunction refers to a switch that is not able to run STP any more, while still forwarding traffic (a brain dead switch).

BPDUs are sent out on all operational network ports, including alternate and backup ports, for each hello time period. Bridge Assurance monitors the receipt of BPDUs on point-to-point links on all network ports. When a port does not receive BPDUs within the allotted hello time period, the port is put into a blocked state (the same as a port inconsistent state, which stops forwarding of frames). When the port resumes receipt of BPDUs, the port resumes normal spanning tree operations.

Only Rapid PVST+ and MST spanning tree protocols support Bridge Assurance. PVST+ does not support Bridge Assurance.

The following example shows how Bridge Assurance protects your network from bridging loops.

The following figure shows a network with normal STP topology.

*Figure 24: Network with Normal STP Topology*

The following figure demonstrates a potential network problem when the device fails (brain dead) and Bridge Assurance is not enabled on the network.
The following figure shows the network with Bridge Assurance enabled, and the STP topology progressing normally with bidirectional BDPUs issuing from every STP network port.

The following figure shows how the potential network problem shown in figure *Network Loop Due to a Malfunctioning Switch* does not occur when you have Bridge Assurance enabled on your network.

The system generates syslog messages when a port is block and unblocked. The following sample output shows the log that is generated for each of these states:
BRIDGE_ASSURANCE_BLOCK

Sep 17 09:48:16.249 PDT: %SPANTREE-2-BRIDGE_ASSURANCE_BLOCK: Bridge Assurance blocking port
GigabitEthernet0/1 on VLAN0001.
Sep 17 09:48:16.249 PDT: %SPANTREE-2-BRIDGE_ASSURANCE_BLOCK: Bridge Assurance blocking port GigabitEthernet1/0/1 on VLAN0001.

BRIDGE_ASSURANCE_UNBLOCK

Sep 17 09:48:58.426 PDT: %SPANTREE-2-BRIDGE_ASSURANCE_UNBLOCK: Bridge Assurance unblocking
port GigabitEthernet0/1 on VLAN0001.
Sep 17 09:48:58.426 PDT: %SPANTREE-2-BRIDGE_ASSURANCE_UNBLOCK: Bridge Assurance unblocking port GigabitEthernet1/0/1 on VLAN0001.

Follow these guidelines when enabling Bridge Assurance:

• It can only be enabled or disabled globally.
• It applies to all operational network ports, including alternate and backup ports.
• Only Rapid PVST+ and MST spanning tree protocols support Bridge Assurance. PVST+ does not support
Bridge Assurance.
• For Bridge Assurance to work properly, it must be supported and configured on both ends of a
point-to-point link. If the device on one side of the link has Bridge Assurance enabled and the device on
the other side does not, the connecting port is blocked and in a Bridge Assurance inconsistent state. We
recommend that you enable Bridge Assurance throughout your network.
• To enable Bridge Assurance on a port, BPDU filtering and BPDU Guard must be disabled.
• You can enable Bridge Assurance in conjunction with Loop Guard.
• You can enable Bridge Assurance in conjunction with Root Guard. The latter is designed to provide a
way to enforce the root bridge placement in the network.

Related Topics

Enabling Bridge Assurance, on page 221

How to Configure Optional Spanning-Tree Features

Enabling PortFast

An interface with the PortFast feature enabled is moved directly to the spanning-tree forwarding state without
waiting for the standard forward-time delay.

If you enable the voice VLAN feature, the PortFast feature is automatically enabled. When you disable voice
VLAN, the PortFast feature is not automatically disabled.

You can enable this feature if your switch is running PVST+, Rapid PVST+, or MSTP.

⚠️ Caution

Use PortFast only when connecting a single end station to an access or trunk port. Enabling this feature on
an interface connected to a switch or hub could prevent spanning tree from detecting and disabling loops in
your network, which could cause broadcast storms and address-learning problems.
This procedure is optional.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **spanning-tree portfast {disable | edge | network}**
5. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Specifies an interface to configure, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 0/2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>spanning-tree portfast {disable</td>
<td>edge</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Enter the following keywords for additional options:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# spanning-tree portfast edge</td>
<td>• Enter disable to disable portfast for the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter edge to enable portfast edge for the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter network to enable portfast network for the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, PortFast is disabled on all interfaces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
What to do next

You can use the `spanning-tree portfast default` global configuration command to globally enable the PortFast feature on all nontrunking ports.

**Related Topics**
- PortFast, on page 196
- Restriction for Optional Spanning-Tree Features, on page 195

---

**Enabling BPDU Guard**

You can enable the BPDU guard feature if your switch is running PVST+, Rapid PVST+, or MSTP.

⚠️ **Caution**

Configure PortFast edge only on ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

This procedure is optional.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `spanning-tree portfast edge`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal          | Enters global configuration mode.                                        |
| Example:                               |                                                                          |
| Switch# `configure terminal`           |                                                                          |

| **Step 3** interface `interface-id`    | Specifies the interface connected to an end station, and enters          |
| Example:                               | interface configuration mode.                                            |
| Switch(config)# `interface gigabitethernet 0/2` |                                                                      |

| **Step 4** spanning-tree portfast edge | Enables the PortFast edge feature.                                      |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# spanning-tree portfast edge</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

#### What to do next

To prevent the port from shutting down, you can use the `errdisable detect cause bpduGuard shutdown vlan` global configuration command to shut down just the offending VLAN on the port where the violation occurred.

You also can use the `spanning-tree bpduGuard enable` interface configuration command to enable BPDU guard on any port without also enabling the PortFast edge feature. When the port receives a BPDU, it is put in the error-disabled state.

**Related Topics**

- [BPDU Guard](#), on page 196

### Enabling BPDU Filtering

You can also use the `spanning-tree bpduFilter enable` interface configuration command to enable BPDU filtering on any interface without also enabling the PortFast edge feature. This command prevents the interface from sending or receiving BPDUs.

**Caution**

Enabling BPDU filtering on an interface is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can enable the BPDU filtering feature if your switch is running PVST+, Rapid PVST+, or MSTP.

**Caution**

Configure PortFast edge only on interfaces that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

This procedure is optional.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `spanning-tree portfast edge bpduFilter default`
4. `interface interface-id`
5. `spanning-tree portfast edge`
6. `end`
# Enabling UplinkFast for Use with Redundant Links

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable  | Enables privileged EXEC mode.  
  Example:  
  Switch> enable  
  • Enter your password if prompted. |
| **Step 2** configure terminal  | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** spanning-tree portfast edge bpdufilter default  | Globally enables BPDU filtering.  
  By default, BPDU filtering is disabled.  
  Example:  
  Switch(config)# spanning-tree portfast edge bpdufilter default |
| **Step 4** interface interface-id  | Specifies the interface connected to an end station, and enters interface configuration mode.  
  Example:  
  Switch(config)# interface gigabitethernet 0/2 |
| **Step 5** spanning-tree portfast edge  | Enables the PortFast edge feature on the specified interface.  
  Example:  
  Switch(config-if)# spanning-tree portfast edge |
| **Step 6** end  | Returns to privileged EXEC mode.  
  Example:  
  Switch(config-if)# end |

### Related Topics

- BPDU Filtering, on page 197

### Enabling UplinkFast for Use with Redundant Links

**Note:**

When you enable UplinkFast, it affects all VLANs on the switch. You cannot configure UplinkFast on an individual VLAN.

You can configure the UplinkFast feature for Rapid PVST+ or for the MSTP, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.
This procedure is optional. Follow these steps to enable UplinkFast and CSUF.

**Before you begin**

UplinkFast cannot be enabled on VLANs that have been configured with a switch priority. To enable UplinkFast on a VLAN with switch priority configured, first restore the switch priority on the VLAN to the default value using the `no spanning-tree vlan vlan-id priority` global configuration command.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. spanning-tree uplinkfast [max-update-rate pkts-per-second]
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree uplinkfast [max-update-rate pkts-per-second]</td>
<td>Enables UplinkFast.</td>
</tr>
<tr>
<td>Example: Switch(config)# spanning-tree uplinkfast max-update-rate 200</td>
<td>(Optional) For <code>pkts-per-second</code>, the range is 0 to 32000 packets per second; the default is 150. If you set the rate to 0, station-learning frames are not generated, and the spanning-tree topology converges more slowly after a loss of connectivity. When you enter this command, CSUF also is enabled on all nonstack port interfaces.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not...
altered). The changes to the switch priority and the path cost reduce the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When you enable the UplinkFast feature using these instructions, CSUF is automatically globally enabled on nonstack port interfaces.

Related Topics
UplinkFast, on page 197
Cross-Stack UplinkFast
How Cross-Stack UplinkFast Works
Events That Cause Fast Convergence

Disabling UplinkFast
This procedure is optional.
Follow these steps to disable UplinkFast and Cross-Stack UplinkFast (CSUF).

**Before you begin**
UplinkFast must be enabled.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **no spanning-tree uplinkfast**
4. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Disables UplinkFast and CSUF on the switch and all of its VLANs.</td>
</tr>
<tr>
<td><strong>no spanning-tree uplinkfast</strong></td>
<td>Switch(config)# no spanning-tree uplinkfast</td>
</tr>
</tbody>
</table>
When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

When you disable the UplinkFast feature using these instructions, CSUF is automatically globally disabled on nonstack port interfaces.

**Enabling BackboneFast**

You can enable BackboneFast to detect indirect link failures and to start the spanning-tree reconfiguration sooner.

You can configure the BackboneFast feature for Rapid PVST+ or for the MSTP, but the feature remains disabled (inactive) until you change the spanning-tree mode to PVST+.

This procedure is optional. Follow these steps to enable BackboneFast on the switch.

**Before you begin**

If you use BackboneFast, you must enable it on all switches in the network. BackboneFast is not supported on Token Ring VLANs. This feature is supported for use with third-party switches.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. spanning-tree backbonefast
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
Enabling EtherChannel Guard

You can enable EtherChannel guard to detect an EtherChannel misconfiguration if your switch is running PVST+, Rapid PVST+, or MSTP.

This procedure is optional.

Follow these steps to enable EtherChannel Guard on the switch.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `spanning-tree etherchannel guard misconfig`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2** | Enters global configuration mode. |
| `configure terminal` | |
| `Switch# configure terminal` | |

| **Step 3** | Enables EtherChannel guard. |
| `spanning-tree etherchannel guard misconfig` | |
| `Switch(config)# spanning-tree etherchannel guard misconfig` | |
### Enabling Root Guard

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. Do not enable the root guard on interfaces to be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and are prevented from reaching the forwarding state.

**Note**

You cannot enable both root guard and loop guard at the same time.

You can enable this feature if your switch is running PVST+, Rapid PVST+, or MSTP.

This procedure is optional.

Follow these steps to enable root guard on the switch.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `spanning-tree guard root`
5. `end`

**What to do next**

You can use the `show interfaces status err-disabled` privileged EXEC command to show which switch ports are disabled because of an EtherChannel misconfiguration. On the remote device, you can enter the `show etherchannel summary` privileged EXEC command to verify the EtherChannel configuration.

After the configuration is corrected, enter the `shutdown` and `no shutdown` interface configuration commands on the port-channel interfaces that were misconfigured.

**Related Topics**

- [EtherChannel Guard](#), on page 201
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies an interface to configure, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> spanning-tree guard root</td>
<td>Enables root guard on the interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>By default, root guard is disabled on all interfaces.</td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree guard root</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- [Root Guard](#), on page 202

### Enabling Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is configured on the entire switched network. Loop guard operates only on interfaces that are considered point-to-point by the spanning tree.

**Note**

You cannot enable both loop guard and root guard at the same time.

You can enable this feature if your switch is running PVST+, Rapid PVST+, or MSTP. This procedure is optional. Follow these steps to enable loop guard on the switch.

### SUMMARY STEPS

1. Enter one of the following commands:
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | Enter one of the following commands:  
- show spanning-tree active  
- show spanning-tree mst | Verifies which interfaces are alternate or root ports. |
| Example: | | |
| | Switch# show spanning-tree active or Switch# show spanning-tree mst | | |
| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | | |
| | Switch# configure terminal | | |
| Step 3 | spanning-tree loopguard default | Enables loop guard. |
| Example: | By default, loop guard is disabled. |
| | Switch(config)# spanning-tree loopguard default | | |
| Step 4 | end | Returns to privileged EXEC mode. |
| Example: | | |
| | Switch(config)# end | | |

**Related Topics**

Loop Guard, on page 203

## Enabling PortFast Port Types

This section describes the different steps to enable Portfast Port types.

**Related Topics**

STP PortFast Port Types, on page 203
Configuring the Default Port State Globally

To configure the default PortFast state, perform this task:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `spanning-tree portfast [edge | network | normal] default`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the default state for all interfaces on the switch. You have these options:</td>
</tr>
<tr>
<td>`spanning-tree portfast [edge</td>
<td>network</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>- (Optional) <code>network</code>—Configures all interfaces as spanning tree network ports. This assumes all ports are connected to switches and bridges. Bridge Assurance is enabled on all network ports by default.</td>
</tr>
<tr>
<td><code>Switch(config)# spanning-tree portfast default</code></td>
<td>- (Optional) <code>normal</code>—Configures all interfaces normal spanning tree ports. These ports can be connected to any type of device.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring PortFast Edge on a Specified Interface

Interfaces configured as edge ports immediately transition to the forwarding state, without passing through the blocking or learning states, on linkup.

**Note**
Because the purpose of this type of port is to minimize the time that access ports must wait for spanning tree to converge, it is most effective when used on access ports. If you enable PortFast edge on a port connecting to another switch, you risk creating a spanning tree loop.

To configure an edge port on a specified interface, perform this task:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-id | port-channel port_channel_number
4. spanning-tree portfast edge [trunk]
5. end
6. show running interface interface-id | port-channel port_channel_number

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies an interface to configure.</td>
</tr>
<tr>
<td>port-channel port_channel_number</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/0/1</td>
<td>port-channel port_channel_number</td>
</tr>
<tr>
<td><strong>Step 4</strong> spanning-tree portfast edge [trunk]</td>
<td>Enables edge behavior on a Layer 2 access port connected to an end workstation or server.</td>
</tr>
<tr>
<td>Example:</td>
<td>• (Optional) <strong>trunk</strong>—Enables edge behavior on a trunk port. Use this keyword if the link is a trunk. Use this command only on ports that are connected to end host devices that terminate VLANs and from which the port should never receive STP BPDUs. Such end host</td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree portfast trunk</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a PortFast Network Port on a Specified Interface

Ports that are connected to Layer 2 switches and bridges can be configured as network ports.

**Note**

Bridge Assurance is enabled only on PortFast network ports. For more information, refer to *Bridge Assurance*.

To configure a port as a network port, perform this task.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id | port-channel port_channel_number`
4. `spanning-tree portfast network`
5. `end`
6. `show running interface interface-id | port-channel port_channel_number`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

- Enter your password if prompted.
### Command or Action | Purpose
--- | ---
**Step 2** configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode.

**Step 3** interface interface-id | port-channel port_channel_number  
Example:  
Switch(config)# interface gigabitethernet 1/0/1 | port-channel port_channel_number | Specifies an interface to configure.

**Step 4** spanning-tree portfast network  
Example:  
Switch(config-if)# spanning-tree portfast network | Enables edge behavior on a Layer 2 access port connected to an end workstation or server.  
- Configures the port as a network port. If you have enabled Bridge Assurance globally, it automatically runs on a spanning tree network port.  
- Use the `no` version of the command to disable PortFast.

**Step 5** end  
Example:  
Switch(config-if)# end | Exits configuration mode.

**Step 6** show running interface interface-id | port-channel port_channel_number  
Example:  
Switch# show running interface gigabitethernet 1/0/1 | port-channel port_channel_number | Verifies the configuration.

### Enabling Bridge Assurance

To configure the Bridge Assurance, perform the steps given below:

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. spanning-tree bridge assurance  
4. end  
5. show spanning-tree summary
### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
Example:  
`Switch> enable` |
| Step 2 | `configure terminal` | Enters global configuration mode.  
Example:  
`Switch# configure terminal` |
| Step 3 | `spanning-tree bridge assurance` | Enables Bridge Assurance on all network ports on the switch.  
Example:  
`Switch(config)# spanning-tree bridge assurance` |
| Step 4 | `end` | Returns to privileged EXEC mode.  
Example:  
`Switch(config)# end` |
| Step 5 | `show spanning-tree summary` | Displays spanning tree information and shows if Bridge Assurance is enabled.  
Example:  
`Switch# show spanning-tree summary` |

### Related Topics

- [Bridge Assurance](#), on page 204

### Examples

#### Examples: Configuring PortFast Edge on a Specified Interface

This example shows how to enable edge behavior on GigabitEthernet interface 1/0/1:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)# end
Switch#
```
This example shows how to verify the configuration:

```
Switch# show running-config interface gigabitethernet1/0/1
Building configuration...
Current configuration:
!
interface GigabitEthernet1/0/1
no ip address
switchport
switchport access vlan 200
switchport mode access
spanning-tree portfast edge
end
```

This example shows how you can display that port GigabitEthernet 1/0/1 is currently in the edge state:

```
Switch# show spanning-tree vlan 200
VLAN0200
Spanning tree enabled protocol rstp
Root ID Priority 2
Address 001b.2a68.5fc0
Cost 3
Port 125 (GigabitEthernet5/9)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 2 (priority 0 sys-id-ext 2)
Address 7010.5c9c.5200
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 0 sec
Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p Edge
```

Examples: Configuring a PortFast Network Port on a Specified Interface

This example shows how to configure GigabitEthernet interface 1/0/1 as a network port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# spanning-tree portfast network
Switch(config-if)# end
Switch#
```

This example shows how to verify the configuration:

```
Switch# show running-config interface gigabitethernet1/0/1
Building configuration...
Current configuration:
!
interface GigabitEthernet1/0/1
no ip address
switchport
switchport access vlan 200
switchport mode access
spanning-tree portfast network
end
```

This example shows the output for show spanning-tree vlan

```
Switch# show spanning-tree vlan
Sep 17 09:51:36.370 PDT: %SYS-5-CONFIG_I: Configured from console by console2

VLAN0002
```
Spanning tree enabled protocol rstp
Root ID Priority 2
Address 7010.5c9c.5200
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 2 (priority 0 sys-id-ext 2)
Address 7010.5c9c.5200
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 0 sec

Interface Role Sts Cost Prio. Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg FWD 4 128.1 P2p Edge
Po4 Desg FWD 3 128.480 P2p Network
Gi4/0/1 Desg FWD 4 128.169 P2p Edge
Gi4/0/47 Desg FWD 4 128.215 P2p Network

Switch#

Example: Configuring Bridge Assurance

This output shows port GigabitEthernet 1/0/1 has been configured as a network port and it is currently in the Bridge Assurance inconsistent state.

The output shows the port type as network and *BA_Inc, indicating that the port is in an inconsistent state.

Switch# show spanning-tree
VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 32778
Address 0002.172c.f400
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)
Address 0002.172c.f400
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio. Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/1 Desg BKN*4 128.270 Network, P2p *BA_Inc

The example shows the output for show spanning-tree summary.

Switch#sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001-VLAN0002, VLAN0128
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is network
Portfast Edge BPDU Guard Default is disabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default is enabled
PVST Simulation Default is enabled but inactive in rapid-pvst mode
Bridge Assurance is enabled
UplinkFast is disabled
BackboneFast is disabled

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
Configured Pathcost method used is short

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN0001</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>VLAN0002</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>VLAN0128</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

3 vlans 0 0 0 13 13

Switch#

**Monitoring the Spanning-Tree Status**

Table 26: Commands for Monitoring the Spanning-Tree Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree active</td>
<td>Displays spanning-tree information on active interfaces only.</td>
</tr>
<tr>
<td>show spanning-tree detail</td>
<td>Displays a detailed summary of interface information.</td>
</tr>
<tr>
<td>show spanning-tree interface <strong>interface-id</strong></td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree mst interface <strong>interface-id</strong></td>
<td>Displays MST information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree summary [totals]</td>
<td>Displays a summary of interface states or displays the total lines of the spanning-tree state section.</td>
</tr>
<tr>
<td>show spanning-tree mst interface <strong>interface-id</strong> portfast edge</td>
<td>Displays spanning-tree portfast information for the specified interface.</td>
</tr>
</tbody>
</table>

**Feature Information for Optional Spanning-Tree Features**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for EtherChannels

- All ports in an EtherChannel must be assigned to the same VLAN or they must be configured as trunk ports.
- When the ports in an EtherChannel are configured as trunk ports, all the ports must be configured with the same mode (IEEE 802.1Q).
Information About EtherChannels

EtherChannel Overview

EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use the EtherChannel to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

An EtherChannel consists of individual Ethernet links bundled into a single logical link.

![Figure 28: Typical EtherChannel Configuration](image)

The EtherChannel provides full-duplex bandwidth up to 8 Gb/s (Gigabit EtherChannel) or 80 Gb/s (10-Gigabit EtherChannel) between your switch and another switch or host.

Each EtherChannel can consist of up to eight compatibly configured Ethernet ports.

The LAN Lite feature set supports up to six EtherChannels. The LAN Base feature set supports up to 24 EtherChannels.

Related Topics
- Configuring Layer 2 EtherChannels, on page 241
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Layer 2 EtherChannel Configuration Guidelines, on page 239

EtherChannel Modes

You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAGP), Link Aggregation Control Protocol (LACP), or On. Configure both ends of the EtherChannel in the same mode:
• When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. If the remote port cannot negotiate an EtherChannel, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

• When you configure an EtherChannel in the on mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the on mode; otherwise, packet loss can occur.

Related Topics
- Configuring Layer 2 EtherChannels, on page 241
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Layer 2 EtherChannel Configuration Guidelines, on page 239

EtherChannel on Switches

You can create an EtherChannel on a switch, on a single switch in the stack, or on multiple switches in the stack (known as cross-stack EtherChannel).

Figure 29: Single-Switch EtherChannel
EtherChannel Link Failover

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

Related Topics
Configuring Layer 2 EtherChannels, on page 241
EtherChannel Configuration Guidelines, on page 238
Default EtherChannel Configuration, on page 237
Layer 2 EtherChannel Configuration Guidelines, on page 239

Channel Groups and Port-Channel Interfaces

An EtherChannel comprises a channel group and a port-channel interface. The channel group binds physical ports to the port-channel interface. Configuration changes applied to the port-channel interface apply to all the physical ports bound together in the channel group.

Figure 31: Relationship of Physical Ports, Channel Group and Port-Channel Interface

The channel-group command binds the physical port and the port-channel interface together. Each EtherChannel has a port-channel logical interface numbered from 1 to 624. This port-channel interface number corresponds to the one specified with the channel-group interface configuration command.
• With Layer 2 ports, use the `channel-group` interface configuration command to dynamically create the port-channel interface.

You also can use the `interface port-channel port-channel-number` global configuration command to manually create the port-channel interface, but then you must use the `channel-group channel-group-number` command to bind the logical interface to a physical port. The `channel-group-number` can be the same as the `port-channel-number`, or you can use a new number. If you use a new number, the `channel-group` command dynamically creates a new port channel.

**Related Topics**

- Creating Port-Channel Logical Interfaces
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Layer 2 EtherChannel Configuration Guidelines, on page 239
- Configuring the Physical Interfaces

**Port Aggregation Protocol**

The Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that can be run only on Cisco switches and on those switches licensed by vendors to support PAgP. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports.

By using PAgP, the switch learns the identity of partners capable of supporting PAgP and the capabilities of each port. It then dynamically groups similarly configured ports (on a single switch) into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, PAgP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, PAgP adds the group to the spanning tree as a single switch port.
PAgP Modes

PAgP modes specify whether a port can send PAgP packets, which start PAgP negotiations, or only respond to PAgP packets received.

Table 27: EtherChannel PAgP Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.</td>
</tr>
<tr>
<td>desirable</td>
<td>Places a port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.</td>
</tr>
</tbody>
</table>

Switch ports exchange PAgP packets only with partner ports configured in the auto or desirable modes. Ports configured in the on mode do not exchange PAgP packets.

Both the auto and desirable modes enable ports to negotiate with partner ports to form an EtherChannel based on criteria such as port speed, and for Layer 2 EtherChannels, based on trunk state and VLAN numbers.

Ports can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:

- A port in the desirable mode can form an EtherChannel with another port that is in the desirable or auto mode.
- A port in the auto mode can form an EtherChannel with another port in the desirable mode.

A port in the auto mode cannot form an EtherChannel with another port that is also in the auto mode because neither port starts PAgP negotiation.

Related Topics
- Configuring Layer 2 EtherChannels, on page 241
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Layer 2 EtherChannel Configuration Guidelines, on page 239
- Creating Port-Channel Logical Interfaces
- Configuring the Physical Interfaces

Silent Mode

If your switch is connected to a partner that is PAgP-capable, you can configure the switch port for nonsilent operation by using the non-silent keyword. If you do not specify non-silent with the auto or desirable mode, silent mode is assumed.

Use the silent mode when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port connected to a silent partner prevents that switch port from ever becoming operational. However, the silent setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.

Related Topics
- Configuring Layer 2 EtherChannels, on page 241
PAgP Learn Method and Priority

Network devices are classified as PAgP physical learners or aggregate-port learners. A device is a physical
learner if it learns addresses by physical ports and directs transmissions based on that knowledge. A device
is an aggregate-port learner if it learns addresses by aggregate (logical) ports. The learn method must be
configured the same at both ends of the link.

When a device and its partner are both aggregate-port learners, they learn the address on the logical port-channel.
The device sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port
learning, it is not important on which physical port the packet arrives.

PAgP cannot automatically detect when the partner device is a physical learner and when the local device is
an aggregate-port learner. Therefore, you must manually set the learning method on the local device to learn
addresses by physical ports. You also must set the load-distribution method to source-based distribution, so
that any given source MAC address is always sent on the same physical port.

You also can configure a single port within the group for all transmissions and use other ports for hot-standby.
The unused ports in the group can be swapped into operation in just a few seconds if the selected single port
loses hardware-signal detection. You can configure which port is always selected for packet transmission by
changing its priority with the `pagp port-priority` interface configuration command. The higher the priority,
the more likely that the port will be selected.

The switch supports address learning only on aggregate ports even though the `physical-port` keyword is
provided in the CLI. The `pagp learn-method` command and the `pagp port-priority` command have no effect
on the switch hardware, but they are required for PAgP interoperability with devices that only support address
learning by physical ports, such as the Catalyst 1900 switch.

When the link partner of the switch is a physical learner, we recommend that you configure the switch as a
physical-port learner by using the `pagp learn-method physical-port` interface configuration command. Set
the load-distribution method based on the source MAC address by using the `port-channel load-balance src-mac`
global configuration command. The switch then sends packets to the physical learner using the same
port in the EtherChannel from which it learned the source address. Only use the `pagp learn-method` command
in this situation.

**Related Topics**

- Configuring the PAgP Learn Method and Priority, on page 245
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Monitoring EtherChannel, PAgP, and LACP Status, on page 255
- Layer 2 EtherChannel Configuration Guidelines, on page 239
PAgP Interaction with Virtual Switches and Dual-Active Detection

A virtual switch can be two or more core switches connected by virtual switch links (VSLs) that carry control and data traffic between them. One of the switches is in active mode. The others are in standby mode. For redundancy, remote switches are connected to the virtual switch by remote satellite links (RSLs).

If the VSL between two switches fails, one switch does not know the status of the other. Both switches could change to the active mode, causing a dual-active situation in the network with duplicate configurations (including duplicate IP addresses and bridge identifiers). The network might go down.

To prevent a dual-active situation, the core switches send PAgP protocol data units (PDUs) through the RSLs to the remote switches. The PAgP PDUs identify the active switch, and the remote switches forward the PDUs to core switches so that the core switches are in sync. If the active switch fails or resets, the standby switch takes over as the active switch. If the VSL goes down, one core switch knows the status of the other and does not change its state.

PAgP Interaction with Other Features

The Dynamic Trunking Protocol (DTP) and the Cisco Discovery Protocol (CDP) send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive PAgP protocol data units (PDUs) on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

PAgP sends and receives PAgP PDUs only from ports that are up and have PAgP enabled for the auto or desirable mode.

Link Aggregation Control Protocol

The LACP is defined in IEEE 802.3ad and enables Cisco switches to manage Ethernet channels between switches that conform to the IEEE 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

By using LACP, the switch learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single switch port.

The independent mode behavior of ports in a port channel is changed. With CSCnt96950, by default, standalone mode is enabled. When no response is received from an LACP peer, ports in the port channel are moved to suspended state.
LACP Modes

LACP modes specify whether a port can send LACP packets or only receive LACP packets.

Table 28: EtherChannel LACP Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.</td>
</tr>
<tr>
<td>passive</td>
<td>Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.</td>
</tr>
</tbody>
</table>

Both the active and passive LACP modes enable ports to negotiate with partner ports to an EtherChannel based on criteria such as port speed, and for Layer 2 EtherChannels, based on trunk state and VLAN numbers.

Ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A port in the active mode can form an EtherChannel with another port that is in the active or passive mode.

- A port in the passive mode cannot form an EtherChannel with another port that is also in the passive mode because neither port starts LACP negotiation.

Related Topics

- Configuring Layer 2 EtherChannels, on page 241
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Layer 2 EtherChannel Configuration Guidelines, on page 239

LACP Interaction with Other Features

The DTP and the CDP send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive LACP PDUs on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

LACP sends and receives LACP PDUs only from ports that are up and have LACP enabled for the active or passive mode.

EtherChannel On Mode

EtherChannel on mode can be used to manually configure an EtherChannel. The on mode forces a port to join an EtherChannel without negotiations. The on mode can be useful if the remote device does not support PAgP or LACP. In the on mode, a usable EtherChannel exists only when the switches at both ends of the link are configured in the on mode.
Ports that are configured in the on mode in the same channel group must have compatible port characteristics, such as speed and duplex. Ports that are not compatible are suspended, even though they are configured in the on mode.

⚠️ Caution
You should use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

EtherChannel Load Deferral Overview

In an Instant Access system, the EtherChannel Load Deferral feature allows ports to be bundled into port channels, but prevents the assignment of group mask values to these ports. This prevents the traffic from being forwarded to new instant access stack members and reduce data loss following a stateful switchover (SSO).

Cisco Catalyst Instant Access creates a single network touch point and a single point of configuration across distribution and access layer switches. Instant Access enables the merging of physical distribution and access layer switches into a single logical entity with a single point of configuration, management, and troubleshooting.

The following illustration represents a sample network where an Instant Access system interacts with a switch (Catalyst 2960-X Series Switches) that is connected via a port channel to stacked clients (Member 1 and Member 2).

When the EtherChannel Load Deferral feature is configured and a new Instant Access client stack member comes up, ports of this newly-joined stack member is bundled into the port channel. In the transition period, the data path is not fully established on the distribution switch (Catalyst 6000 Series Switches), and traffic originating from the access layer switch (Catalyst 2960-X Series Switches) reaches the non-established ports and the traffic gets lost.

When load share deferral is enabled on a port channel, the assignment of a member port’s load share is delayed for a period that is configured globally by the `port-channel load-defer` command. During the deferral period, the load share of a deferred member port is set to 0. In this state, the deferred port is capable of receiving data and control traffic, and of sending control traffic, but the port is prevented from sending data traffic to the virtual switching system (VSS). Upon expiration of the global deferral timer, the deferred member port exits the deferral state and the port assumes its normal configured load share.

Load share deferral is applied only if at least one member port of the port channel is currently active with a nonzero load share. If a port enabled for load share deferral is the first member bringing up the EtherChannel, the deferral feature does not apply and the port will forward traffic immediately.

This feature is enabled on a per port-channel basis; however, the load deferral timer is configured globally and not per port-channel. As a result, when a new port is bundled, the timer starts only if it is not already running. If some other ports are already deferred then the new port will be deferred only for the remaining amount of time.

The load deferral is stopped as soon as a member in one of the deferred port channels is unbundled. As a result, all the ports that were deferred is assigned a group-mask in the event of an unbundling during the deferral period.

⚠️ Note
When you try to enable this feature on a stack member switch, the following message is displayed:

`Load share deferral is supported only on stand-alone stack.`
Default EtherChannel Configuration

The default EtherChannel configuration is described in this table.

**Table 29: Default EtherChannel Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel groups</td>
<td>None assigned.</td>
</tr>
<tr>
<td>Port-channel logical interface</td>
<td>None defined.</td>
</tr>
<tr>
<td>PAgP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>PAgP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>PAgP priority</td>
<td>128 on all ports.</td>
</tr>
<tr>
<td>LACP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>LACP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>LACP port priority</td>
<td>32768 on all ports.</td>
</tr>
<tr>
<td>LACP system priority</td>
<td>32768.</td>
</tr>
<tr>
<td>LACP system ID</td>
<td>LACP system priority and the switch or stack MAC address.</td>
</tr>
<tr>
<td>Load-balancing</td>
<td>Load distribution on the switch is based on the source-MAC address of the incoming packet.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Layer 2 EtherChannels, on page 241
- EtherChannel Overview, on page 228
- EtherChannel Modes, on page 228
- EtherChannel on Switches, on page 229
- EtherChannel Link Failover, on page 230
- LACP Modes, on page 235
- PAgP Modes, on page 232
- Silent Mode, on page 232
- Creating Port-Channel Logical Interfaces
- Channel Groups and Port-Channel Interfaces, on page 230
- Configuring the Physical Interfaces
- Configuring EtherChannel Load-Balancing
- Configuring the PAgP Learn Method and Priority, on page 245
- PAgP Learn Method and Priority, on page 233
- Configuring the LACP System Priority, on page 247
- Configuring the LACP Port Priority, on page 248
EtherChannel Configuration Guidelines

If improperly configured, some EtherChannel ports are automatically disabled to avoid network loops and other problems. Follow these guidelines to avoid configuration problems:

- Configure a PAgP EtherChannel with up to eight Ethernet ports of the same type.
- Configure a LACP EtherChannel with up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.
- Configure all ports in an EtherChannel to operate at the same speeds and duplex modes.
- Enable all ports in an EtherChannel. A port in an EtherChannel that is disabled by using the `shutdown` interface configuration command is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.
- When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, you must also make the changes to all ports in the group:
  - Allowed-VLAN list
  - Spanning-tree path cost for each VLAN
  - Spanning-tree port priority for each VLAN
  - Spanning-tree Port Fast setting
- Do not configure a port to be a member of more than one EtherChannel group.
- Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.
- Do not configure a secure port as part of an EtherChannel or the reverse.
- Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.
- If EtherChannels are configured on switch interfaces, remove the EtherChannel configuration from the interfaces before globally enabling IEEE 802.1x on a switch by using the `dot1x system-auth-control` global configuration command.
- Do not enable link-state tracking on individual interfaces that will be part of a downstream Etherchannel interface.

Related Topics

- Configuring Layer 2 EtherChannels, on page 241
- EtherChannel Overview, on page 228
- EtherChannel Modes, on page 228
- EtherChannel on Switches, on page 229
- EtherChannel Link Failover, on page 230
- LACP Modes, on page 235
- PAgP Modes, on page 232
Layer 2 EtherChannel Configuration Guidelines

When configuring Layer 2 EtherChannels, follow these guidelines:

- Assign all ports in the EtherChannel to the same VLAN, or configure them as trunks. Ports with different native VLANs cannot form an EtherChannel.

- An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAGP is set to the auto or desirable mode.

- Ports with different spanning-tree path costs can form an EtherChannel if they are otherwise compatibly configured. Setting different spanning-tree path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.

Related Topics

- Configuring Layer 2 EtherChannels
- EtherChannel Overview
- EtherChannel Modes
- EtherChannel on Switches
- EtherChannel Link Failover
- LACP Modes
- PAGP Modes
- Silent Mode
- Creating Port-Channel Logical Interfaces
- Channel Groups and Port-Channel Interfaces
- Configuring the Physical Interfaces
- Configuring EtherChannel Load-Balancing
- Configuring the PAGP Learn Method and Priority
- PAGP Learn Method and Priority
- Configuring the LACP System Priority
- Configuring the LACP Port Priority

Auto-LAG

The auto-LAG feature provides the ability to auto create EtherChannels on ports connected to a switch. By default, auto-LAG is disabled globally and is enabled on all port interfaces. The auto-LAG applies to a switch only when it is enabled globally.
On enabling auto-LAG globally, the following scenarios are possible:

- All port interfaces participate in creation of auto EtherChannels provided the partner port interfaces have EtherChannel configured on them. For more information, see the "The supported auto-LAG configurations between the actor and partner devices" table below.

- Ports that are already part of manual EtherChannels cannot participate in creation of auto EtherChannels.

- When auto-LAG is disabled on a port interface that is already a part of an auto created EtherChannel, the port interface will unbundle from the auto EtherChannel.

The following table shows the supported auto-LAG configurations between the actor and partner devices:

### Table 30: The supported auto-LAG configurations between the actor and partner devices

<table>
<thead>
<tr>
<th>Actor/Partner</th>
<th>Active</th>
<th>Passive</th>
<th>Auto</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Passive</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Auto</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

On disabling auto-LAG globally, all auto created Etherchannels become manual EtherChannels.

You cannot add any configurations in an existing auto created EtherChannel. To add, you should first convert it into a manual EtherChannel by executing the `port-channel <channel-number> persistent`.

**Note**

Auto-LAG uses the LACP protocol to create auto EtherChannel. Only one EtherChannel can be automatically created with the unique partner devices.

**Related Topics**

- Configuring Auto-LAG Globally, on page 252
- Configuring Auto LAG: Examples, on page 257
- Configuring Auto-LAG on a Port Interface, on page 253
- Configuring Persistence with Auto-LAG, on page 254
- Auto-LAG Configuration Guidelines, on page 240

### Auto-LAG Configuration Guidelines

Follow these guidelines when configuring the auto-LAG feature.

- When auto-LAG is enabled globally and on the port interface, and if you do not want the port interface to become a member of the auto EtherChannel, disable the auto-LAG on the port interface.

- A port interface will not bundle to an auto EtherChannel when it is already a member of a manual EtherChannel. To allow it to bundle with the auto EtherChannel, first unbundle the manual EtherChannel on the port interface.

- When auto-LAG is enabled and auto EtherChannel is created, you can create multiple EtherChannels manually with the same partner device. But by default, the port tries to create auto EtherChannel with the partner device.
- The auto-LAG is supported only on Layer 2 EtherChannel. It is not supported on Layer 3 interface and Layer 3 EtherChannel.

**Related Topics**
- Configuring Auto-LAG Globally, on page 252
- Configuring Auto LAG: Examples, on page 257
- Configuring Auto-LAG on a Port Interface, on page 253
- Configuring Persistence with Auto-LAG, on page 254
- Auto-LAG, on page 239

## How to Configure EtherChannels

After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface, and configuration changes applied to the physical port affect only the port where you apply the configuration.

### Configuring Layer 2 EtherChannels

You configure Layer 2 EtherChannels by assigning ports to a channel group with the `channel-group` interface configuration command. This command automatically creates the port-channel logical interface.

#### SUMMARY STEPS

1. `configure terminal`
2. `interface interface-id`
3. `switchport mode {access | trunk}`
4. `switchport access vlan vlan-id`
5. `channel-group channel-group-number mode {auto [non-silent] | desirable [non-silent] | on } | { active | passive}
6. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
**Example:**
Switch# configure terminal | Enters global configuration mode. |
| **Step 2**
**Example:**
Switch(config)# interface gigabitethernet1/0/10 | Specifies a physical port, and enters interface configuration mode. Valid interfaces are physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. |
**Command or Action** | **Purpose**
--- | ---
For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

### Step 3

```bash
switchport mode \{access | trunk\}
```

**Example:**

```bash
Switch(config-if)# switchport mode access
```

Assigns all ports as static-access ports in the same VLAN, or configure them as trunks.

If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.

### Step 4

```bash
switchport access vlan vlan-id
```

**Example:**

```bash
Switch(config-if)# switchport access vlan 22
```

(Optional) If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.

### Step 5

```bash
channel-group \(channel-group-number\) mode \{auto [non-silent] | desirable [non-silent] | on \} | \{active | passive\}
```

**Example:**

```bash
Switch(config-if)# channel-group 5 mode auto
```

Assigns the port to a channel group, and specifies the PAgP or the LACP mode.

For `channel-group-number`, the range is 1 to 24.

For `channel-group-number`, the range is 1 to 6.

For `mode`, select one of these keywords:

- **auto** — Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This keyword is not supported when EtherChannel members are from different switches in the switch stack.

- **desirable** — Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. This keyword is not supported when EtherChannel members are from different switches in the switch stack.

- **on** — Forces the port to channel without PAgP or LACP. In the `on` mode, an EtherChannel exists only when a port group in the `on` mode is connected to another port group in the `on` mode.

- **non-silent** — (Optional) If your switch is connected to a partner that is PAgP-capable, configures the switch port for nonsilent operation when the port is in the `auto` or `desirable` mode. If you do not specify `non-silent`, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.
### Configuring Port Channel Load Deferral

#### SUMMARY STEPS

1. enable
2. configure terminal
3. port-channel load-defer seconds
4. interface type number
5. port-channel load-defer
6. end
7. show etherchannel channel-group port-channel
8. show platform pm group-masks

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• active—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.</td>
<td></td>
</tr>
<tr>
<td>• passive—Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Example:**

```
Switch(config-if)# end
```

---

**Related Topics**

- [EtherChannel Overview](#), on page 228
- [EtherChannel Modes](#), on page 228
- [EtherChannel on Switches](#), on page 229
- [EtherChannel Link Failover](#), on page 230
- [LACP Modes](#), on page 235
- [PAgP Modes](#), on page 232
- [Silent Mode](#), on page 232
- [EtherChannel Configuration Guidelines](#), on page 238
- [Default EtherChannel Configuration](#), on page 237
- [Layer 2 EtherChannel Configuration Guidelines](#), on page 239
# Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> port-channel load-defer <code>seconds</code></td>
<td>Configures the port load share deferral interval for all port channels.</td>
</tr>
<tr>
<td>Example: Switch(config)# port-channel load-defer 60</td>
<td>• <code>seconds</code>—The time interval during which load sharing is initially 0 for deferred port channels. The range is 1 to 1800 seconds; the default is 120 seconds</td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type number</td>
<td>Configures a port channel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface port-channel 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> port-channel load-defer</td>
<td>Enables port load share deferral on the port channel.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# port-channel load-defer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show etherchannel channel-group port-channel</td>
<td>Displays port channel information.</td>
</tr>
<tr>
<td>Example: Switch# show etherchannel 1 port-channel</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> show platform pm group-masks</td>
<td>Display EtherChannel group masks information.</td>
</tr>
<tr>
<td>Example: Switch# show platform pm group-masks</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

The following is sample output from the `show etherchannel channel-group port-channel` command. If the `channel-group` argument is not specified; the command displays information about all channel groups are displayed.

```
Switch# show etherchannel 1 port-channel

Port-channels in the group:

```

---

Layer 2

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
Port-channel: Po1
------------
Age of the Port-channel = 0d:00h:37m:08s
Logical slot/port = 9/1  Number of ports = 0
GC = 0x00000000  HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = -
Port security = Disabled
Load share deferral = Enabled  defer period = 120 sec  time left = 0 sec

The following is sample output from the `show platform pm group-masks` command. Deferred ports have the group mask of 0xFFFF, when the defer timer is running.

```
Switch# show platform pm group-masks
```

<table>
<thead>
<tr>
<th>Group</th>
<th>#ports</th>
<th>Group frame-dist</th>
<th>slot</th>
<th>port</th>
<th>mask</th>
<th>interface</th>
<th>index</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
<td></td>
<td>src-mac</td>
<td>Gi1/0/12</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
<td>src-mac</td>
<td>Gi1/0/10</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td></td>
<td></td>
<td>src-mac</td>
<td>Gi1/0/11</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>8</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>9</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>10</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>11</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>12</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>13</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>14</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>15</td>
<td></td>
<td></td>
<td>src-mac</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring the PAgP Learn Method and Priority

This task is optional.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `pagp learn-method physical-port`
4. `pagp port-priority priority`
5. `end`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** interface interface-id | Specifies the port for transmission, and enters interface configuration mode. |
| Example: Switch(config)# interface gigabitethernet 1/0/20/2 | |

| **Step 3** pagp learn-method physical-port | Selects the PAgP learning method. By default, **aggregation-port learning** is selected, which means the switch sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives. Selects physical-port to connect with another switch that is a physical learner. The learning method must be configured the same at both ends of the link. |
| Example: Switch(config-if)# pagp learn-method physical port | |

| **Step 4** pagp port-priority priority | Assigns a priority so that the selected port is chosen for packet transmission. For priority, the range is 0 to 255. The default is 128. The higher the priority, the more likely that the port will be used for PAgP transmission. |
| Example: Switch(config-if)# pagp port-priority 200 | |

| **Step 5** end | Returns to privileged EXEC mode. |
| Example: Switch(config-if)# end | |

**Related Topics**

- PAgP Learn Method and Priority, on page 233
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Monitoring EtherChannel, PAgP, and LACP Status, on page 255
- Layer 2 EtherChannel Configuration Guidelines, on page 239
Configuring LACP Hot-Standby Ports

When enabled, LACP tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 16 ports. Only eight LACP links can be active at one time. The software places any additional links in a hot-standby mode. If one of the active links becomes inactive, a link that is in the hot-standby mode becomes active in its place.

If you configure more than eight links for an EtherChannel group, the software automatically decides which of the hot-standby ports to make active based on the LACP priority. To every link between systems that operate LACP, the software assigns a unique priority made up of these elements (in priority order):

- LACP system priority
- System ID (the switch MAC address)
- LACP port priority
- Port number

In priority comparisons, numerically lower values have higher priority. The priority decides which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

Determining which ports are active and which are hot standby is a two-step procedure. First the system with a numerically lower system priority and system ID is placed in charge of the decision. Next, that system decides which ports are active and which are hot standby, based on its values for port priority and port number. The port priority and port number values for the other system are not used.

You can change the default values of the LACP system priority and the LACP port priority to affect how the software selects active and standby links.

Configuring the LACP System Priority

You can configure the system priority for all the EtherChannels that are enabled for LACP by using the `lacp system-priority` global configuration command. You cannot configure a system priority for each LACP-configured channel. By changing this value from the default, you can affect how the software selects active and standby links.

You can use the `show etherchannel summary` privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

Follow these steps to configure the LACP system priority. This procedure is optional.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `lacp system-priority` *priority*
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring the LACP Port Priority

By default, all ports use the same port priority. If the local system has a lower value for the system priority and the system ID than the remote system, you can affect which of the hot-standby links become active first by changing the port priority of LACP EtherChannel ports to a lower value than the default. The hot-standby ports that have lower port numbers become active in the channel first. You can use the `show etherchannel summary` privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

#### Related Topics
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Layer 2 EtherChannel Configuration Guidelines, on page 239
- Monitoring EtherChannel, PAgP, and LACP Status, on page 255

#### Configuring the LACP Port Priority

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Example:**  
Switch> `enable` | • Enter your password if prompted. |
| **Step 2**  
**Example:**  
Switch# `configure terminal` | Enters global configuration mode. |
| **Step 3**  
**Example:**  
Switch(config)# `lacp system-priority priority` | Configures the LACP system priority.  
The range is 1 to 65535. The default is 32768.  
The lower the value, the higher the system priority. |
| **Step 4**  
**Example:**  
Switch(config)# `end` | Returns to privileged EXEC mode. |

#### Note
If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), all the ports that cannot be actively included in the EtherChannel are put in the hot-standby state and are used only if one of the channeled ports fails.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `lacp port-priority priority`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable
Example: `Switch> enable` | Enables privileged EXEC mode.
- Enter your password if prompted. |
| **Step 2** `configure terminal`  
Example: `Switch# configure terminal` | Enters global configuration mode. |
| **Step 3** `interface interface-id`  
Example: `Switch(config)# interface gigabitethernet 1/0/20/2` | Specifies the port to be configured, and enters interface configuration mode. |
| **Step 4** `lacp port-priority priority`  
Example: `Switch(config-if)# lacp port-priority 32000` | Configures the LACP port priority.  
The range is 1 to 65535. The default is 32768. The lower the value, the more likely that the port will be used for LACP transmission. |
| **Step 5** `end`  
Example: `Switch(config-if)# end` | Returns to privileged EXEC mode. |

**Related Topics**
- EtherChannel Configuration Guidelines, on page 238
- Default EtherChannel Configuration, on page 237
- Layer 2 EtherChannel Configuration Guidelines, on page 239
- Monitoring EtherChannel, PAgP, and LACP Status, on page 255
Configuring the LACP Port Channel Min-Links Feature

You can specify the minimum number of active ports that must be in the link-up state and bundled in an EtherChannel for the port channel interface to transition to the link-up state. Using EtherChannel min-links, you can prevent low-bandwidth LACP EtherChannels from becoming active. Port channel min-links also cause LACP EtherChannels to become inactive if they have too few active member ports to supply the required minimum bandwidth.

To configure the minimum number of links that are required for a port channel. Perform the following tasks.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface port-channel *channel-number*
4. port-channel min-links *min-links-number*
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface port-channel <em>channel-number</em></td>
<td>Enters interface configuration mode for a port-channel. For <em>channel-number</em>, the range is 1 to 6.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface port-channel 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> port-channel min-links <em>min-links-number</em></td>
<td>Specifies the minimum number of member ports that must be in the link-up state and bundled in the EtherChannel for the port channel interface to transition to the link-up state. For <em>min-links-number</em>, the range is 2 to 8.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# port-channel min-links 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring LACP Fast Rate Timer

You can change the LACP timer rate to modify the duration of the LACP timeout. Use the `lacp rate` command to set the rate at which LACP control packets are received by an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port`
4. `lacp rate {normal | fast}`
5. `end`
6. `show lacp internal`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`interface {fastethernet</td>
<td>gigabitethernet</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>interface gigabitEthernet 2/1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>`lacp rate {normal</td>
<td>fast}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# <code>lacp rate fast</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
**Configuring Auto-LAG Globally**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. [no] port-channel auto
4. end
5. show etherchannel auto

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] port-channel auto</td>
<td>Enables the auto-LAG feature on a switch globally. Use the no form of this command to disable the auto-LAG feature on the switch globally.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>Note</strong> By default, the auto-LAG feature is enabled on the port.</td>
</tr>
<tr>
<td>Switch(config)# port-channel auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Auto-LAG on a Port Interface

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `[no] channel-group auto`
5. `end`
6. `show etherchannel auto`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enablen</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 1/0/10/1</td>
</tr>
</tbody>
</table>
Configuring Persistence with Auto-LAG

You use the persistence command to convert the auto created EtherChannel into a manual one and allow you to add configuration on the existing EtherChannel.

SUMMARY STEPS

1. enable
2. port-channel channel-number persistent
3. show etherchannel summary

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 port-channel channel-number persistent</td>
<td>Converts the auto created EtherChannel into a manual one and allows you to add configuration on the EtherChannel.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# port-channel 1 persistent</td>
<td></td>
</tr>
</tbody>
</table>

### Step 3

**Switch# show etherchannel summary**

**Example:**

Switch# show etherchannel summary

### Related Topics

- Configuring Auto-LAG Globally, on page 252
- Auto-LAG, on page 239
- Auto-LAG Configuration Guidelines, on page 240
- Configuring Auto-LAG on a Port Interface, on page 253
- Configuring Auto LAG: Examples, on page 257

## Monitoring EtherChannel, PAgP, and LACP Status

You can display EtherChannel, PAgP, and LACP status using the commands listed in this table.

**Table 31: Commands for Monitoring EtherChannel, PAgP, and LACP Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lACP { channel-group-number counters</td>
<td>Clears LACP channel-group information and traffic counters.</td>
</tr>
<tr>
<td>clear PAgP { channel-group-number counters</td>
<td>Clears PAgP channel-group information and traffic counters.</td>
</tr>
<tr>
<td>show etherchannel [ channel-group-number [ detail</td>
<td>Displays EtherChannel information in a brief, detailed, and one-line summary form. Also displays the load-balance or frame-distribution scheme, port, port-channel, protocol, and Auto-LAG information.</td>
</tr>
<tr>
<td>show PAgP [ channel-group-number ] { counters</td>
<td>Displays PAgP information such as traffic information, the internal PAgP configuration, and neighbor information.</td>
</tr>
<tr>
<td>show PAgP [ channel-group-number ] dual-active</td>
<td>Displays the dual-active detection status.</td>
</tr>
<tr>
<td>show LACP [ channel-group-number ] { counters</td>
<td>Displays LACP information such as traffic information, the internal LACP configuration, and neighbor information.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verifies your configuration entries.</td>
</tr>
<tr>
<td>show etherchannel load-balance</td>
<td>Displays the load balance or frame distribution scheme among ports in the port channel.</td>
</tr>
</tbody>
</table>
Configuration Examples for Configuring EtherChannels

Configuring Layer 2 EtherChannels: Examples

This example shows how to configure an EtherChannel on a single switch. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/10/1-2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single switch. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the LACP mode active:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet2/0/10/1-2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

PoE or LACP negotiation errors may occur if you configure two ports from switch to the access point (AP). This scenario can be avoided if the port channel configuration is on the switch side. For more details, see the following example:

```
interface Port-channel1
    switchport access vlan 20
    switchport mode access
    switchport nonegotiate
    no port-channel standalone-disable    <-this one
    spanning-tree portfast
```

**Note**

If the port reports LACP errors on port flap, you should include the following command as well: `no errdisable detect cause pagp-flap`
Example: Configuring Port Channel Load Deferral

Switch# configure terminal
Switch(config)# port-channel load-defer 60
Switch(config)# interface port-channel 10
Switch(config-if)# port-channel load-defer
Switch(config-if)# end

Configuring Auto LAG: Examples

This example shows how to configure Auto-LAG on a switch

switch> enable
switch# configure terminal
switch (config)# port-channel auto
switch (config-if)# end
switch# show etherchannel auto

The following example shows the summary of EtherChannel that was created automatically.

switch# show etherchannel auto
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
+-----------------------------------------+----------------+---------------------------------------------------+
| 1 Po1(SUA) LACP Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P) |
+-----------------------------------------+----------------+---------------------------------------------------+

The following example shows the summary of auto EtherChannel after executing the `port-channel 1 persistent` command.

switch# port-channel 1 persistent
switch# show etherchannel summary
switch# show etherchannel summary

The following example shows the summary of auto EtherChannel after executing the `port-channel 1 persistent` command.

switch# port-channel 1 persistent
switch# show etherchannel summary
switch# show etherchannel summary

Number of channel-groups in use: 1
Number of aggregators: 1
### Configuring LACP Port Channel Min-Links: Examples

This example shows how to configure LACP port-channel min-links:

```
switch > enable
switch# configure terminal
switch(config)# interface port-channel 5
switch(config-if)# port-channel min-links 3
switch(config-if)# show etherchannel 5 summary
switch# end
```

When the minimum links requirement is not met in standalone switches, the port-channel is flagged and assigned SM/SN or RM/RN state.

```
switch# show etherchannel 5 summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use N- not in use, no aggregation
f - failed to allocate aggregator
M - not in use, no aggregation due to minimum links not met
m - not in use, port not aggregated due to minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
D - default port
Number of channel-groups in use: 6
Number of aggregators: 6
```

```
Group  Port-channel  Protocol  Ports
--+------------------------+-----------------------------+
 6  Po25 (RM)  LACP  Gi1/3/1(D) Gi1/3/2(D) Gi2/2/25(D) Gi2/2/26(W)
```

### Related Topics
- Configuring the LACP Port Channel Min-Links Feature, on page 250

---

### Example: Configuring LACP Fast Rate Timer

This example shows you how to configure the LACP rate:

```
switch> enable
switch# configure terminal
switch(config)# interface gigabitEthernet 2/1
switch(config-if)# lACP rate fast
switch(config-if)# exit
switch(config)# end
switch# show lacp internal
```

---

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
switch# show lacp counters

The following is sample output from the `show lacp internal` command:

```
switch# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode   P - Device is in Passive mode
Channel group 6
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Te1/49 FA bndl 32768 0x19 0x19 0x32 0x3F
Te1/50 FA bndl 32768 0x19 0x19 0x33 0x3F
Te1/51 FA bndl 32768 0x19 0x19 0x34 0x3F
Te1/52 FA bndl 32768 0x19 0x19 0x35 0x3F
```

The following is sample output from the `show lacp counters` command:

```
switch# show lacp counters
LACPDU Marker Marker Response LACPDU
Port Sent Recv Sent Recv Sent Recv Pkts Err
---------------------------------------------------------------------
Channel group: 6
Te1/1/27 2 2 0 0 0 0 0
Te2/1/25 2 2 0 0 0 0 0
```

Related Topics

- Configuring LACP Fast Rate Timer, on page 251

### Additional References for EtherChannels

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 command reference</td>
<td>Catalyst 2960-X Switch Layer 2 Command Reference</td>
</tr>
</tbody>
</table>

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for EtherChannels

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(3)E2, Cisco IOS XE 3.7.2E</td>
<td>Auto-LAG feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 14

Configuring the MAC Address-Table Move Update Feature

- Finding Feature Information, on page 261
- Information About MAC Address-Table Move Update, on page 261
- How to Configure MAC Address-Table Move Update, on page 263
- Monitoring the MAC Address-Table Move Update, on page 265
- Configuration Examples for MAC Address-Table Move Update, on page 265

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About MAC Address-Table Move Update

MAC Address-Table Move Update

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence when a primary (forwarding) link goes down and the standby link begins forwarding traffic.

Figure 32: MAC Address-Table Move Update Example

In the following figure, switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and D through a Flex Links pair. Port 1 is forwarding traffic, and port 2 is in the backup state. Traffic from the PC to the server is forwarded from port 1 to port 3. The MAC address of the PC has been...
learned on port 3 of switch C. Traffic from the server to the PC is forwarded from port 3 to port 1.

If the MAC address-table move update feature is not configured and port 1 goes down, port 2 starts forwarding traffic. However, for a short time, switch C keeps forwarding traffic from the server to the PC through port 3, and the PC does not get the traffic because port 1 is down. If switch C removes the MAC address of the PC on port 3 and relears it on port 4, traffic can then be forwarded from the server to the PC through port 2.

If the MAC address-table move update feature is configured and enabled on the switches, and port 1 goes down, port 2 starts forwarding traffic from the PC to the server. The switch sends a MAC address-table move update packet from port 2. Switch C gets this packet on port 4 and immediately learns the MAC address of the PC on port 4, which reduces the reconvergence time.

You can configure the access switch, switch A, to send MAC address-table move update messages. You can also configure the uplink switches B, C, and D to get and process the MAC address-table move update messages. When switch C gets a MAC address-table move update message from switch A, switch C learns the MAC address of the PC on port 4. Switch C updates the MAC address table, including the forwarding table entry for the PC.

Switch A does not need to wait for the MAC address-table update. The switch detects a failure on port 1 and immediately starts forwarding server traffic from port 2, the new forwarding port. This change occurs in less than 100 milliseconds (ms). The PC is directly connected to switch A, and the connection status does not change. Switch A does not need to update the PC entry in the MAC address table.
Related Topics
Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages, on page 264
Configuring MAC Address-Table Move Update, on page 263
Configuring the MAC Address-Table Move Update: Examples, on page 265

MAC Address-Table Move Update Configuration Guidelines

• You can enable and configure this feature on the access switch to send the MAC address-table move updates.
• You can enable and configure this feature on the uplink switches to get the MAC address-table move updates.

How to Configure MAC Address-Table Move Update

Configuring MAC Address-Table Move Update

SUMMARY STEPS
1. configure terminal
2. interface interface-id
3. Use one of the following:
   • switchport backup interface interface-id
   • switchport backup interface interface-id mmu primary vlan vlan-id
4. end
5. mac address-table move update transmit
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch#interface gigabitethernet1/0/1</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages

#### SUMMARY STEPS

1. configure terminal
2. mac address-table move update receive
3. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode</td>
</tr>
</tbody>
</table>

---

**Related Topics**

- Configuring the MAC Address-Table Move Update: Examples, on page 265
- MAC Address-Table Move Update, on page 261

---

**Layer 2**

---

**Purpose**

- Configures a physical Layer 2 interface (or port channel), as part of a Flex Links pair with the interface. The MAC address-table move update VLAN is the lowest VLAN ID on the interface.
- Configure a physical Layer 2 interface (or port channel) and specifies the VLAN ID on the interface, which is used for sending the MAC address-table move update.
- When one link is forwarding traffic, the other interface is in standby mode.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• switchport backup interface interface-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• switchport backup interface interface-id mmu</td>
<td></td>
</tr>
<tr>
<td></td>
<td>primary vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# switchport backup interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>gigabitethernet0/2 mmu primary vlan 2</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

Switch(config-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2

---

**Step 4**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to global configuration mode</td>
</tr>
</tbody>
</table>

**Example:**

Switch(config-if)# end

---

**Step 5**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac address-table move update transmit</td>
<td>Enables the access switch to send MAC address-table move update updates to other switches in the network if the primary link goes down and the switch starts forwarding traffic through the standby link.</td>
</tr>
</tbody>
</table>

**Example:**

Switch(config)# mac address-table move update transmit

---

**Step 6**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode</td>
</tr>
</tbody>
</table>

**Example:**

Switch(config)# end
Purpose

Command or Action

Example:
Switch# configure terminal

Step 2
mac address-table move update receive

Example:
Switch (config)# mac address-table move update receive

Step 3
end

Example:
Switch (config)# end

Related Topics

- Configuring the MAC Address-Table Move Update: Examples, on page 265
- MAC Address-Table Move Update, on page 261

Monitoring the MAC Address-Table Move Update

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac address-table move update</td>
<td>Displays the MAC address-table move update information on the switch.</td>
</tr>
</tbody>
</table>

Configuration Examples for MAC Address-Table Move Update

Configuring the MAC Address-Table Move Update: Examples

This example shows how to verify the configuration after you configure an access switch to send MAC address-table move updates:

Switch# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None

Related Topics
- Configuring MAC Address-Table Move Update, on page 263
- Configuring a Switch to Obtain and Process MAC Address-Table Move Update Messages, on page 264
- MAC Address-Table Move Update, on page 261
CHAPTER 15

Configuring UniDirectional Link Detection

- Finding Feature Information, on page 267
- Restrictions for Configuring UDLD, on page 267
- Information About UDLD, on page 268
- How to Configure UDLD, on page 270
- Monitoring and Maintaining UDLD, on page 273
- Additional References for UDLD, on page 273
- Feature Information for UDLD, on page 274

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring UDLD

The following are restrictions for configuring UniDirectional Link Detection (UDLD):

- A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.

Caution

Loop guard works only on point-to-point links. We recommend that each end of the link has a directly connected device that is running STP.
Information About UDLD

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected ports on fiber-optic links.

In normal and aggressive modes, UDLD works with the Layer 1 mechanisms to learn the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

Normal Mode

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic port are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the ports are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In this case, the logical link is considered undetermined, and UDLD does not disable the port.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up because the Layer 1 mechanisms detects a physical problem with the link. In this case, UDLD does not take any action and the logical link is considered undetermined.

Related Topics
- Enabling UDLD Globally, on page 270
- Enabling UDLD on an Interface, on page 272

Aggressive Mode

In aggressive mode, UDLD detects a unidirectional link by using the previous detection methods. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of these problems exists:

- On fiber-optic or twisted-pair links, one of the ports cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the ports is down while the other is up.
- One of the fiber strands in the cable is disconnected.
In these cases, UDLD disables the affected port.

In a point-to-point link, UDLD hello packets can be considered as a heartbeat whose presence guarantees the health of the link. Conversely, the loss of the heartbeat means that the link must be shut down if it is not possible to reestablish a bidirectional link.

If both fiber strands in a cable are working normally from a Layer 1 perspective, UDLD in aggressive mode detects whether those fiber strands are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation because autonegotiation operates at Layer 1.

Related Topics
- Enabling UDLD Globally, on page 270
- Enabling UDLD on an Interface, on page 272

**Methods to Detect Unidirectional Links**

UDLD operates by using two methods:
- Neighbor database maintenance
- Event-driven detection and echoing

Related Topics
- Enabling UDLD Globally, on page 270
- Enabling UDLD on an Interface, on page 272

**Neighbor Database Maintenance**

UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active port to keep each device informed about its neighbors.

When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

Whenever a port is disabled and UDLD is running, whenever UDLD is disabled on a port, or whenever the switch is reset, UDLD clears all existing cache entries for the ports affected by the configuration change. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

**Event-Driven Detection and Echoing**

UDLD relies on echoing as its detection operation. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the port is disabled.

Related Topics
- Enabling UDLD Globally, on page 270
Enabling UDLD on an Interface, on page 272

UDLD Reset Options

If an interface becomes disabled by UDLD, you can use one of the following options to reset UDLD:

- The **udld reset** interface configuration command.
- The **shutdown** interface configuration command followed by the **no shutdown** interface configuration command restarts the disabled port.
- The **no udld {aggressive | enable}** global configuration command followed by the **udld {aggressive | enable}** global configuration command reenables the disabled ports.
- The **no udld port** interface configuration command followed by the **udld port [aggressive]** interface configuration command reenables the disabled fiber-optic port.
- The **errdisable recovery cause udld** global configuration command enables the timer to automatically recover from the UDLD error-disabled state, and the **errdisable recovery interval interval** global configuration command specifies the time to recover from the UDLD error-disabled state.

Related Topics

- Enabling UDLD Globally, on page 270
- Enabling UDLD on an Interface, on page 272

Default UDLD Configuration

*Table 32: Default UDLD Configuration*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDLD global enable state</td>
<td>Globally disabled</td>
</tr>
<tr>
<td>UDLD per-port enable state for fiber-optic media</td>
<td>Disabled on all Ethernet fiber-optic ports</td>
</tr>
<tr>
<td>UDLD per-port enable state for twisted-pair (copper) media</td>
<td>Disabled on all Ethernet 10/100 and 1000BASE-TX ports</td>
</tr>
<tr>
<td>UDLD aggressive mode</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Related Topics

- Enabling UDLD Globally, on page 270
- Enabling UDLD on an Interface, on page 272

How to Configure UDLD

Enabling UDLD Globally

Follow these steps to enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports on the switch.
SUMMARY STEPS

1. configure terminal
2. udld {aggressive | enable | message time message-timer-interval}
3. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 udld {aggressive</td>
<td>enable</td>
</tr>
<tr>
<td>Example: Switch(config)# udld enable message time 10</td>
<td>- aggressive—Enables UDLD in aggressive mode on all fiber-optic ports.</td>
</tr>
<tr>
<td></td>
<td>- enable—Enables UDLD in normal mode on all fiber-optic ports on the switch. UDLD is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>An individual interface configuration overrides the setting of the udld enable global configuration command.</td>
</tr>
<tr>
<td></td>
<td>- message time message-timer-interval—Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. The range is from 1 to 90 seconds; the default value is 15.</td>
</tr>
<tr>
<td></td>
<td>Note This command affects fiber-optic ports only. Use the udld interface configuration command to enable UDLD on other port types.</td>
</tr>
<tr>
<td></td>
<td>Use the no form of this command, to disable UDLD.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Monitoring and Maintaining UDLD
- Aggressive Mode, on page 268
- Normal Mode, on page 268
Enabling UDLD on an Interface

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `udld port [aggressive]`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the port to be enabled for UDLD, and enters interface</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 1/0/10/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>UDLD is disabled by default.</td>
</tr>
<tr>
<td><code>udld port [aggressive]</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# udld port aggressive</code></td>
<td>(Optional) Enables UDLD in aggressive mode on the specified port.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
Related Topics
- Monitoring and Maintaining UDLD
- Aggressive Mode, on page 268
- Normal Mode, on page 268
- Methods to Detect Unidirectional Links, on page 269
- Event-Driven Detection and Echoing, on page 269
- UDLD Reset Options, on page 270
- Default UDLD Configuration, on page 270

Monitoring and Maintaining UDLD

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show udld [interface-id</td>
<td>neighbors]`</td>
</tr>
</tbody>
</table>

Additional References for UDLD

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 command reference</td>
<td>Catalyst 2960-X Switch Layer 2 Command Reference</td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for UDLD

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART V

Network Management

- Configuring Cisco IOS Configuration Engine, on page 277
- Configuring the Cisco Discovery Protocol, on page 289
- Configuring Simple Network Management Protocol, on page 301
- Configuring SPAN, on page 327
Prerequisites for Configuring the Configuration Engine

- Obtain the name of the configuration engine instance to which you are connecting.

- Because the CNS uses both the event bus and the configuration server to provide configurations to devices, you must define both ConfigID and Device ID for each configured switch.

- All switches configured with the `cns config partial` global configuration command must access the event bus. The DeviceID, as originated on the switch, must match the DeviceID of the corresponding switch definition in the Cisco Configuration Engine. You must know the hostname of the event bus to which you are connecting.

Restrictions for Configuring the Configuration Engine

- Within the scope of a single instance of the configuration server, no two configured switches can share the same value for ConfigID.

- Within the scope of a single instance of the event bus, no two configured switches can share the same value for DeviceID.
Information About Configuring the Configuration Engine

Cisco Configuration Engine Software

The Cisco Configuration Engine is network management utility software that acts as a configuration service for automating the deployment and management of network devices and services. Each Cisco Configuration Engine manages a group of Cisco devices (switches and routers) and the services that they deliver, storing their configurations and delivering them as needed. The Cisco Configuration Engine automates initial configurations and configuration updates by generating device-specific configuration changes, sending them to the device, executing the configuration change, and logging the results.

The Cisco Configuration Engine supports standalone and server modes and has these Cisco Networking Services (CNS) components:

- Configuration service:
  - Web server
  - File manager
  - Namespace mapping server

- Event service (event gateway)
- Data service directory (data models and schema)

In standalone mode, the Cisco Configuration Engine supports an embedded directory service. In this mode, no external directory or other data store is required. In server mode, the Cisco Configuration Engine supports the use of a user-defined external directory.

*Figure 33: Cisco Configuration Engine Architectural Overview*
Configuration Service

The Configuration Service is the core component of the Cisco Configuration Engine. It consists of a Configuration Server that works with Cisco IOS CNS agents on the switch. The Configuration Service delivers device and service configurations to the switch for initial configuration and mass reconfiguration by logical groups. Switches receive their initial configuration from the Configuration Service when they start up on the network for the first time.

The Configuration Service uses the CNS Event Service to send and receive configuration change events and to send success and failure notifications.

The Configuration Server is a web server that uses configuration templates and the device-specific configuration information stored in the embedded (standalone mode) or remote (server mode) directory.

Configuration templates are text files containing static configuration information in the form of CLI commands. In the templates, variables are specified by using Lightweight Directory Access Protocol (LDAP) URLs that reference the device-specific configuration information stored in a directory.

The Cisco IOS agent can perform a syntax check on received configuration files and publish events to show the success or failure of the syntax check. The configuration agent can either apply configurations immediately or delay the application until receipt of a synchronization event from the configuration server.

Event Service

The Cisco Configuration Engine uses the Event Service for receipt and generation of configuration events. The Event Service consists of an event agent and an event gateway. The event agent is on the switch and facilitates the communication between the switch and the event gateway on the Cisco Configuration Engine.

The Event Service is a highly capable publish-and-subscribe communication method. The Event Service uses subject-based addressing to send messages to their destinations. Subject-based addressing conventions define a simple, uniform namespace for messages and their destinations.

NameSpace Mapper

The Cisco Configuration Engine includes the NameSpace Mapper (NSM) that provides a lookup service for managing logical groups of devices based on application, device or group ID, and event.

Cisco IOS devices recognize only event subject-names that match those configured in Cisco IOS software; for example, cisco.cns.config.load. You can use the namespace mapping service to designate events by using any desired naming convention. When you have populated your data store with your subject names, NSM changes your event subject-name strings to those known by Cisco IOS.

For a subscriber, when given a unique device ID and event, the namespace mapping service returns a set of events to which to subscribe. Similarly, for a publisher, when given a unique group ID, device ID, and event, the mapping service returns a set of events on which to publish.

Cisco Networking Services IDs and Device Hostnames

The Cisco Configuration Engine assumes that a unique identifier is associated with each configured switch. This unique identifier can take on multiple synonyms, where each synonym is unique within a particular namespace. The event service uses namespace content for subject-based addressing of messages.
The Cisco Configuration Engine intersects two namespaces, one for the event bus and the other for the configuration server. Within the scope of the configuration server namespace, the term ConfigID is the unique identifier for a device. Within the scope of the event bus namespace, the term DeviceID is the CNS unique identifier for a device.

**ConfigID**

Each configured switch has a unique ConfigID, which serves as the key into the Cisco Configuration Engine directory for the corresponding set of switch CLI attributes. The ConfigID defined on the switch must match the ConfigID for the corresponding switch definition on the Cisco Configuration Engine.

The ConfigID is fixed at startup time and cannot be changed until the device restarts, even if the switch hostname is reconfigured.

**DeviceID**

Each configured switch participating on the event bus has a unique DeviceID, which is analogous to the switch source address so that the switch can be targeted as a specific destination on the bus.

The origin of the DeviceID is defined by the Cisco IOS hostname of the switch. However, the DeviceID variable and its usage reside within the event gateway adjacent to the switch.

The logical Cisco IOS termination point on the event bus is embedded in the event gateway, which in turn functions as a proxy on behalf of the switch. The event gateway represents the switch and its corresponding DeviceID to the event bus.

The switch declares its hostname to the event gateway immediately after the successful connection to the event gateway. The event gateway couples the DeviceID value to the Cisco IOS hostname each time this connection is established. The event gateway retains this DeviceID value for the duration of its connection to the switch.

**Hostname and DeviceID**

The DeviceID is fixed at the time of the connection to the event gateway and does not change even when the switch hostname is reconfigured.

When changing the switch hostname on the switch, the only way to refresh the DeviceID is to break the connection between the switch and the event gateway. For instructions on refreshing DeviceIDs, see "Related Topics."

When the connection is reestablished, the switch sends its modified hostname to the event gateway. The event gateway redefines the DeviceID to the new value.

**Caution**

When using the Cisco Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the switch acquires after, not before, and you must reinitialize the configuration for your Cisco IOS CNS agent. Otherwise, subsequent partial configuration command operations may malfunction.

**Hostname, DeviceID, and ConfigID**

In standalone mode, when a hostname value is set for a switch, the configuration server uses the hostname as the DeviceID when an event is sent on hostname. If the hostname has not been set, the event is sent on the cn=<value> of the device.
In server mode, the hostname is not used. In this mode, the unique DeviceID attribute is always used for sending an event on the bus. If this attribute is not set, you cannot update the switch.

These and other associated attributes (tag value pairs) are set when you run Setup on the Cisco Configuration Engine.

**Automated CNS Configuration**

To enable automated CNS configuration of the switch, you must first complete the prerequisites listed in this topic. When you complete them, power on the switch. At the setup prompt, do nothing; the switch begins the initial configuration. When the full configuration file is loaded on your switch, you do not need to do anything else.

For more information on what happens during initial configuration, see "Related Topics."

**Table 33: Prerequisites for Enabling Automatic Configuration**

<table>
<thead>
<tr>
<th>Device</th>
<th>Required Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access switch</td>
<td>Factory default (no configuration file)</td>
</tr>
<tr>
<td>Distribution switch</td>
<td>• IP helper address</td>
</tr>
<tr>
<td></td>
<td>• Enable DHCP relay agent&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>• IP routing (if used as default gateway)</td>
</tr>
<tr>
<td>DHCP server</td>
<td>• IP address assignment</td>
</tr>
<tr>
<td></td>
<td>• TFTP server IP address</td>
</tr>
<tr>
<td></td>
<td>• Path to bootstrap configuration file on the TFTP server</td>
</tr>
<tr>
<td></td>
<td>• Default gateway IP address</td>
</tr>
<tr>
<td>TFTP server</td>
<td>• A bootstrap configuration file that includes the CNS configuration commands that enable the switch to communicate with the Configuration Engine</td>
</tr>
<tr>
<td></td>
<td>• The switch configured to use either the switch MAC address or the serial number (instead of the default hostname) to generate the ConfigID and EventID</td>
</tr>
<tr>
<td></td>
<td>• The CNS event agent configured to push the configuration file to the switch</td>
</tr>
<tr>
<td>CNS Configuration Engine</td>
<td>One or more templates for each type of device, with the ConfigID of the device mapped to the template.</td>
</tr>
</tbody>
</table>

<sup>2</sup> A DHCP Relay is needed only when the DHCP Server is on a different subnet from the client.
How to Configure the Configuration Engine

Enabling the CNS Event Agent

Note
You must enable the CNS event agent on the switch before you enable the CNS configuration agent.

Follow these steps to enable the CNS event agent on the switch.

SUMMARY STEPS

1. enable
2. configure terminal
3. cns event {hostname | ip-address} [port-number] [keepalive seconds retry-count] [failover-time seconds] [reconnect-time time] | backup
4. end
5. show running-config
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> cns event {hostname</td>
<td>ip-address} [port-number] [keepalive seconds retry-count] [failover-time seconds] [reconnect-time time]</td>
</tr>
<tr>
<td>Example: Switch(config)# cns event 10.180.1.27 keepalive 120 10</td>
<td>• For {hostname</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For port number, enter the port number for the event gateway. The default port number is 11011.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For keepalive seconds, enter how often the switch sends keepalive messages. For retry-count, enter the number of unanswered keepalive messages that the switch sends before the connection is terminated. The default for each is 0.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
| **Purpose** | • (Optional) For failover-time seconds, enter how long the switch waits for the primary gateway route after the route to the backup gateway is established.  
• (Optional) For reconnect-time time, enter the maximum time interval that the switch waits before trying to reconnect to the event gateway.  
• (Optional) Enter backup to show that this is the backup gateway. (If omitted, this is the primary gateway.)  

**Note** Though visible in the command-line help string, the encrypt and the clock-timeout time keywords are not supported.  

**Step 4** end  
**Example:**  
Switch(config)# end  

**Step 5** show running-config  
**Example:**  
Switch# show running-config  

**Step 6** copy running-config startup-config  
**Example:**  
Switch# copy running-config startup-config  

What to do next

To verify information about the event agent, use the show cns event connections command in privileged EXEC mode.

To disable the CNS event agent, use the no cns event { ip-address | hostname } global configuration command.

### Refreshing DeviceIDs

Follow these steps to refresh a DeviceID when changing the hostname on the switch.

**SUMMARY STEPS**

1. enable  
2. show cns config connections
3. Make sure that the CNS event agent is properly connected to the event gateway.
4. `show cns event connections`
5. Record from the output of Step 4 the information for the currently connected connection listed below. You will be using the IP address and port number in subsequent steps of these instructions.
6. `configure terminal`
7. `no cns event ip-address port-number`
8. `cns event ip-address port-number`
9. `end`
10. Make sure that you have reestablished the connection between the switch and the event connection by examining the output from `show cns event connections`.
11. `show running-config`
12. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enable privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Displays whether the CNS event agent is connecting to the gateway, connected, or active, and the gateway used by the event agent, its IP address and port number. |
| *Example:* | | |
| `show cns config connections` | `Switch# show cns config connections` | |

| **Step 3** | Make sure that the CNS event agent is properly connected to the event gateway. |
| | Examine the output of `show cns config connections` for the following: |
| | • Connection is active. |
| | • Connection is using the currently configured switch hostname. The DeviceID will be refreshed to correspond to the new hostname configuration using these instructions. |

| **Step 4** | Displays the event connection information for your switch. |
| *Example:* | `Switch# show cns event connections` | |

| **Step 5** | Record from the output of Step 4 the information for the currently connected connection listed below. You will be using the IP address and port number in subsequent steps of these instructions. |

| **Step 6** | Enters global configuration mode. |
| *Example:* | | |
### Monitoring CNS Configurations

#### Table 34: CNS show Commands

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch# configure terminal</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Specify the IP address and port number that you recorded in Step 5 in this command.</td>
</tr>
<tr>
<td><strong>no cns event ip-address port-number</strong></td>
<td>This command breaks the connection between the switch and the event gateway. It is necessary to first break, then reestablish, this connection to refresh the DeviceID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Switch(config)# no cns event 172.28.129.22 2012</strong></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Specify the IP address and port number that you recorded in Step 5 in this command.</td>
</tr>
<tr>
<td><strong>cns event ip-address port-number</strong></td>
<td>This command reestablishes the connection between the switch and the event gateway.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Switch(config)# cns event 172.28.129.22 2012</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>end</strong></td>
<td><strong>Switch(config)# end</strong></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Make sure that you have reestablished the connection between the switch and the event connection by examining the output from <code>show cns event connections</code>.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>show running-config</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Switch# show running-config</strong></td>
<td><strong>Switch# show running-config</strong></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>copy running-config startup-config</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Switch# copy running-config startup-config</strong></td>
<td><strong>Switch# copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>
### Command | Purpose
--- | ---
**show cns config outstanding** | Displays information about incremental (partial) CNS configurations that have started but are not yet completed.
Switch# `show cns config outstanding`

**show cns config stats** | Displays statistics about the Cisco IOS CNS agent.
Switch# `show cns config stats`

**show cns event connections** | Displays the status of the CNS event agent connections.
Switch# `show cns event connections`

**show cns event gateway** | Displays the event gateway information for your switch.
Switch# `show cns event gateway`

**show cns event stats** | Displays statistics about the CNS event agent.
Switch# `show cns event stats`

**show cns event subject** | Displays a list of event agent subjects that are subscribed to by applications.
Switch# `show cns event subject`

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
| Configuration Engine Setup | *Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux*

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>
Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for the Configuration Engine

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
Feature History and Information for the Configuration Engine
CHAPTER 17

Configuring the Cisco Discovery Protocol

- Finding Feature Information, on page 289
- Information About CDP, on page 289
- How to Configure CDP, on page 290
- Monitoring and Maintaining CDP, on page 298
- Additional References, on page 299
- Feature History and Information for Cisco Discovery Protocol, on page 300

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About CDP

CDP Overview

CDP is a device discovery protocol that runs over Layer 2 (the data-link layer) on all Cisco-manufactured devices (routers, bridges, access servers, controllers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information,
which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

On the switch, CDP enables Network Assistant to display a graphical view of the network. The switch uses CDP to find cluster candidates and maintain information about cluster members and other devices up to three cluster-enabled devices away from the command switch by default.

Related Topics
- Configuring CDP Characteristics, on page 290
- Monitoring and Maintaining CDP, on page 298

Default CDP Configuration

This table shows the default CDP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP global state</td>
<td>Enabled</td>
</tr>
<tr>
<td>CDP interface state</td>
<td>Enabled</td>
</tr>
<tr>
<td>CDP timer (packet update frequency)</td>
<td>60 seconds</td>
</tr>
<tr>
<td>CDP holdtime (before discarding)</td>
<td>180 seconds</td>
</tr>
<tr>
<td>CDP Version-2 advertisements</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Related Topics
- Enabling CDP, on page 293
- Disabling CDP, on page 292
- Enabling Cisco Discovery Protocol on an Interface, on page 296
- Disabling Cisco Discovery Protocol on an Interface, on page 295

How to Configure CDP

Configuring CDP Characteristics

You can configure these CDP characteristics:

- Frequency of CDP updates
- Amount of time to hold the information before discarding it
- Whether or not to send Version-2 advertisements

Note
Steps 3 through 5 are all optional and can be performed in any order.

Follow these steps to configure the CDP characteristics.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `cdp timer seconds`
4. `cdp holdtime seconds`
5. `cdp advertise-v2`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `enable` | Enables privileged EXEC mode.  
   **Example:**  
   `Switch> enable`  
   • Enter your password if prompted. |
| **Step 2** | `configure terminal` | Enters global configuration mode.  
   **Example:**  
   `Switch# configure terminal` |
| **Step 3** | `cdp timer seconds` | (Optional) Sets the transmission frequency of CDP updates in seconds.  
   **Example:**  
   `Switch(config)# cdp timer 20`  
   The range is 5 to 254; the default is 60 seconds. |
| **Step 4** | `cdp holdtime seconds` | (Optional) Specifies the amount of time a receiving device should hold the information sent by your device before discarding it.  
   **Example:**  
   `Switch(config)# cdp holdtime 60`  
   The range is 10 to 255 seconds; the default is 180 seconds. |
| **Step 5** | `cdp advertise-v2` | (Optional) Configures CDP to send Version-2 advertisements.  
   **Example:**  
   `Switch(config)# cdp advertise-v2`  
   This is the default state. |
| **Step 6** | `end` | Returns to privileged EXEC mode.  
   **Example:**  
   `Switch(config)# end` |
| **Step 7** | `show running-config` | Verifies your entries.  
   **Example:** |
### Purpose

**Command or Action**  
Switch# show running-config

**Step 8**  
- **copy running-config startup-config**
  
**Example:**
  
Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

### What to do next

Use the **no** form of the CDP commands to return to the default settings.

**Related Topics**
- CDP Overview, on page 289
- Monitoring and Maintaining CDP, on page 298

### Disabling CDP

CDP is enabled by default.

**Note**

Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages. Disabling CDP can interrupt cluster discovery and device connectivity.

Follow these steps to disable the CDP device discovery capability.

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. no cdp run  
4. end  
5. show running-config  
6. copy running-config startup-config

**DETAILS STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
  - enable  
  - Example:  
    
  Switch> enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
</table>
| Enters global configuration mode. | configure terminal  
Example: Switch# configure terminal |
| Disables CDP. | no cdp run  
Example: Switch(config)# no cdp run |
| Returns to privileged EXEC mode. | end  
Example: Switch(config)# end |
| Verifies your entries. | show running-config  
Example: Switch# show running-config |
| (Optional) Saves your entries in the configuration file. | copy running-config startup-config  
Example: Switch# copy running-config startup-config |

**What to do next**

You must reenable CDP to use it.

**Related Topics**

- Enabling CDP, on page 293
- Default CDP Configuration, on page 290

**Enabling CDP**

CDP is enabled by default.

**Note**

Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages. Disabling CDP can interrupt cluster discovery and device connectivity.

Follow these steps to enable CDP when it has been disabled.
Before you begin
CDP must be disabled, or it cannot be enabled.

SUMMARY STEPS
1. enable
2. configure terminal
3. cdp run
4. end
5. show running-config
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  
  Example: 
  Switch> enable
| Enables privileged EXEC mode.    |
|                                 |  
  • Enter your password if prompted. |
| **Step 2**
  
  Example: 
  Switch# configure terminal
| Enters global configuration mode. |
| **Step 3**
  
  Example: 
  Switch(config)# cdp run
| Enables CDP if it has been disabled. |
| **Step 4**
  
  Example: 
  Switch(config)# end
| Returns to privileged EXEC mode. |
| **Step 5**
  
  Example: 
  Switch# show running-config
| Verifies your entries. |
| **Step 6**
  
  Example: 
  Switch# copy running-config startup-config
| (Optional) Saves your entries in the configuration file. |
What to do next

Use the `show run all` command to show that CDP has been enabled. If you enter only `show run`, the enabling of CDP may not be displayed.

**Related Topics**
- Default CDP Configuration, on page 290
- Disabling CDP, on page 292

---

## Disabling Cisco Discovery Protocol on an Interface

Cisco Discovery Protocol is enabled by default on all supported interfaces to send and to receive Cisco Discovery Protocol information.

---

**Note**

Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

**Note**

Cisco Discovery Protocol bypass is not supported and may cause a port go into err-disabled state.

---

Follow these steps to disable Cisco Discovery Protocol on a port.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `no cdp enable`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 3**

*interface interface-id*

**Example:**

Switch(config)# interface gigabitethernet 0/1

*Purpose*

Specifies the interface on which you are disabling Cisco Discovery Protocol, and enters interface configuration mode.

**Step 4**

no cdp enable

**Example:**

Switch(config-if)# no cdp enable

*Purpose*

Disables Cisco Discovery Protocol on the interface specified in Step 3.

**Step 5**

end

**Example:**

Switch(config)# end

*Purpose*

Returns to privileged EXEC mode.

**Step 6**

show running-config

**Example:**

Switch# show running-config

*Purpose*

Verifies your entries.

**Step 7**

copy running-config startup-config

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

### Related Topics

- [Enabling Cisco Discovery Protocol on an Interface](#)
- Default CDP Configuration

---

### Enabling Cisco Discovery Protocol on an Interface

Cisco Discovery Protocol is enabled by default on all supported interfaces to send and to receive Cisco Discovery Protocol information.

---

**Note**

Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

---

**Note**

Cisco Discovery Protocol bypass is not supported and may cause a port go into err-disabled state.

Follow these steps to enable Cisco Discovery Protocol on a port on which it has been disabled.
Before you begin
Cisco Discovery Protocol must be disabled on the port that you are trying to Cisco Discovery Protocol enable on, or it cannot be enabled.

SUMMARY STEPS
1. enable
2. configure terminal
3. interface interface-id
4. cdp enable
5. end
6. show running-config
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the interface on which you are enabling Cisco Discovery Protocol, and enters interface configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# interface gigabitethernet0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> cdp enable</td>
<td>Enables Cisco Discovery Protocol on a disabled interface.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config-if)# cdp enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><em>Example:</em> Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>
## Monitoring and Maintaining CDP

### Table 35: Commands for Displaying CDP Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear cdp counters</code></td>
<td>Resets the traffic counters to zero.</td>
</tr>
<tr>
<td><code>clear cdp table</code></td>
<td>Deletes the CDP table of information about neighbors.</td>
</tr>
<tr>
<td><code>show cdp</code></td>
<td>Displays global information, such as frequency of transmissions and the holdtime for packets being sent.</td>
</tr>
<tr>
<td><code>show cdp entry entry-name [version] [protocol]</code></td>
<td>Displays information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor about which you want information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.</td>
</tr>
<tr>
<td><code>show cdp interface [interface-id]</code></td>
<td>Displays information about interfaces where CDP is enabled. You can limit the display to the interface about which you want information.</td>
</tr>
<tr>
<td><code>show cdp neighbors [interface-id] [detail]</code></td>
<td>Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.</td>
</tr>
<tr>
<td><code>show cdp traffic</code></td>
<td>Displays CDP counters, including the number of packets sent and received and checksum errors.</td>
</tr>
</tbody>
</table>
### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management Commands</td>
<td><em>Network Management Command Reference, Cisco IOS Release 15.2(2)E</em></td>
</tr>
</tbody>
</table>

#### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
# Feature History and Information for Cisco Discovery Protocol

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
</tbody>
</table>
CHAPTER 18

Configuring Simple Network Management Protocol

• Finding Feature Information, on page 301
• Prerequisites for SNMP, on page 301
• Restrictions for SNMP, on page 303
• Information About SNMP, on page 304
• How to Configure SNMP, on page 308
• Monitoring SNMP Status, on page 322
• SNMP Examples, on page 323
• Additional References, on page 324
• Feature History and Information for Simple Network Management Protocol, on page 325

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SNMP

Supported SNMP Versions

This software release supports the following SNMP versions:

• SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.

• SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:
• SNMPv2—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.

• SNMPv2C—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.

• SNMPv3—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
  • Message integrity—Ensures that a packet was not tampered with in transit.
  • Authentication—Determines that the message is from a valid source.
  • Encryption—Mixes the contents of a package to prevent it from being read by an unauthorized source.

To select encryption, enter the `priv` keyword.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent’s MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval function and more detailed error message reporting to management stations. The bulk retrieval function retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security method is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

The following table identifies characteristics and compares different combinations of security models and levels:

<table>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv2C</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>Model</td>
<td>Level</td>
<td>Authentication</td>
<td>Encryption</td>
<td>Result</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------------------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>authNoPriv</td>
<td>Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)</td>
<td>No</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>authPriv</td>
<td>MD5 or SHA</td>
<td>Data Encryption Standard (DES) or Advanced Encryption Standard (AES)</td>
<td>Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 3DES 168-bit encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- AES 128-bit, 192-bit, or 256-bit encryption</td>
</tr>
</tbody>
</table>

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, SNMPv2C, or SNMPv3.

**Restrictions for SNMP**

**Version Restrictions**

- SNMPv1 does not support informs.
Information About SNMP

SNMP Overview

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB). The SNMP manager can be part of a network management system (NMS) such as Cisco Prime Infrastructure. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in the following table:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-request</td>
<td>Retrieves a value from a specific variable.</td>
</tr>
<tr>
<td>get-next-request</td>
<td>Retrieves a value from a variable within a table.</td>
</tr>
<tr>
<td>get-bulk-request</td>
<td>Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data.</td>
</tr>
<tr>
<td>get-response</td>
<td>Replies to a get-request, get-next-request, and set-request sent by an NMS.</td>
</tr>
<tr>
<td>set-request</td>
<td>Stores a value in a specific variable.</td>
</tr>
<tr>
<td>trap</td>
<td>An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.</td>
</tr>
</tbody>
</table>

With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.

The get-bulk command only works with SNMPv2 or later.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

A community string can have one of the following attributes:

- Read-only (RO)—Gives all objects in the MIB except the community strings read access to authorized management stations, but does not allow write access.
- Read-write (RW)—Gives all objects in the MIB read and write access to authorized management stations, but does not allow access to the community strings.
- When a cluster is created, the command switch manages the exchange of messages among member switches and the SNMP application. The Network Assistant software appends the member switch number (@esN, where N is the switch number) to the first configured RW and RO community strings on the command switch and propagates them to the member switches.

**Related Topics**
- Configuring Community Strings, on page 309

SNMP MIB Variables Access

An example of an NMS is the Cisco Prime Infrastructure network management software. Cisco Prime Infrastructure 2.0 software uses the switch MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in the figure, the SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in get-request, get-next-request, and set-request format.
SNMP Notifications

SNMP allows the switch to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps or informs, or both. Use the `snmp-server host` command to specify whether to send SNMP notifications as traps or informs.

**Note**

SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be resent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the switch and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be resent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the switch is a concern and notification is not required, use traps.

**Related Topics**

- [Configuring SNMP Notifications](#), on page 315
- [Monitoring SNMP Status](#), on page 322

SNMP ifIndex MIB Object Values

In an NMS, the IF-MIB generates and assigns an interface index (ifIndex) object value that is a unique number greater than zero to identify a physical or a logical interface. When the switch reboots or the switch software is upgraded, the switch uses this same value for the interface. For example, if the switch assigns a port 2 an ifIndex value of 10003, this value is the same after the switch reboots.

The switch uses one of the values in the following table to assign an ifIndex value to an interface:

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>ifIndex Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVI</td>
<td>1–4999</td>
</tr>
<tr>
<td>EtherChannel</td>
<td>5001–5048</td>
</tr>
</tbody>
</table>
**Interface Type** | **iFIndex Range**
--- | ---
Tunnel | 5078–5142
Physical (such as Gigabit Ethernet or SFP-module interfaces) based on type and port numbers | 10000–14500
Null | 14501
Loopback and Tunnel | 24567+

5 SVI = switch virtual interface
6 SFP = small form-factor pluggable

**Default SNMP Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP agent</td>
<td>Disabled(^2)</td>
</tr>
<tr>
<td>SNMP trap receiver</td>
<td>None configured.</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>None enabled except the trap for TCP connections (tty).</td>
</tr>
<tr>
<td>SNMP version</td>
<td>If no version keyword is present, the default is Version 1.</td>
</tr>
<tr>
<td>SNMPv3 authentication</td>
<td>If no keyword is entered, the default is the noauth (noAuthNoPriv) security level.</td>
</tr>
<tr>
<td>SNMP notification type</td>
<td>If no type is specified, all notifications are sent.</td>
</tr>
</tbody>
</table>

\(^7\) This is the default when the switch starts and the startup configuration does not have any `snmp-server` global configuration commands.

**SNMP Configuration Guidelines**

If the switch starts and the switch startup configuration has at least one `snmp-server` global configuration command, the SNMP agent is enabled.

An SNMP group is a table that maps SNMP users to SNMP views. An SNMP user is a member of an SNMP group. An SNMP host is the recipient of an SNMP trap operation. An SNMP engine ID is a name for the local or remote SNMP engine.

When configuring SNMP, follow these guidelines:

- When configuring an SNMP group, do not specify a notify view. The `snmp-server host` global configuration command auto-generates a notify view for the user and then adds it to the group associated with that user. Modifying the group's notify view affects all users associated with that group.

- To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

- Before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID` global configuration command with the `remote` option. The remote agent's SNMP engine ID and user password are used to compute the authentication and privacy digests. If you do not configure the remote engine ID first, the configuration command fails.
• When configuring SNMP informs, you need to configure the SNMP engine ID for the remote agent in the SNMP database before you can send proxy requests or informs to it.

• If a local user is not associated with a remote host, the switch does not send informs for the auth (authNoPriv) and the priv (authPriv) authentication levels.

• Changing the value of the SNMP engine ID has significant results. A user's password (entered on the command line) is converted to an MD5 or SHA security digest based on the password and the local engine ID. The command-line password is then destroyed, as required by RFC 2274. Because of this deletion, if the value of the engine ID changes, the security digests of SNMPv3 users become invalid, and you need to reconfigure SNMP users by using the `snmp-server user username` global configuration command. Similar restrictions require the reconfiguration of community strings when the engine ID changes.

**Related Topics**

- Configuring SNMP Groups and Users, on page 312
- Monitoring SNMP Status, on page 322

## How to Configure SNMP

### Disabling the SNMP Agent

The `no snmp-server` global configuration command disables all running versions (Version 1, Version 2C, and Version 3) of the SNMP agent on the device. You reenable all versions of the SNMP agent by the first `snmp-server` global configuration command that you enter. There is no Cisco IOS command specifically designated for enabling SNMP.

Follow these steps to disable the SNMP agent.

**Before you begin**

The SNMP Agent must be enabled before it can be disabled. The SNMP agent is enabled by the first `snmp-server` global configuration command entered on the device.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `no snmp-server`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code> Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>Enter your password if prompted.</em></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>no snmp-server</td>
<td>Disables the SNMP agent operation.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# no snmp-server</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- SNMP Agent Functions, on page 304
- Monitoring SNMP Status, on page 322

## Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent
- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community
Follow these steps to configure a community string on the switch.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. snmp-server community string [view view-name] [ro | rw] [access-list-number]
4. access-list access-list-number {deny | permit} source [source-wildcard]
5. end
6. show running-config
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server community string [view view-name] [ro</td>
<td>rw] [access-list-number]</td>
</tr>
<tr>
<td>Example: Switch(config)# snmp-server community comaccess ro 4</td>
<td>Note: The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.</td>
</tr>
<tr>
<td></td>
<td>- For <strong>string</strong>, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <strong>view</strong>, specify the view record accessible to the community.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) Specify either read-only (<strong>ro</strong>) if you want authorized management stations to retrieve MIB objects, or specify read-write (<strong>rw</strong>) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <strong>access-list-number</strong>, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.</td>
</tr>
</tbody>
</table>
### Purpose

If you specified an IP standard access list number in Step 3, then create the list, repeating the command as many times as necessary.

- For **access-list-number**, enter the access list number specified in Step 3.
- The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched.
- For **source**, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent.
- (Optional) For **source-wildcard**, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.

Recall that the access list is always terminated by an implicit deny statement for everything.

### Command or Action

#### Step 4

| access-list access-list-number {deny | permit} source [source-wildcard] |
|-----------------------------|

**Example:**

```
Switch(config)# access-list 4 deny any
```

#### Step 5

<table>
<thead>
<tr>
<th>end</th>
</tr>
</thead>
</table>

**Example:**

```
Switch(config)# end
```

#### Step 6

<table>
<thead>
<tr>
<th>show running-config</th>
</tr>
</thead>
</table>

**Example:**

```
Switch# show running-config
```

#### Step 7

<table>
<thead>
<tr>
<th>copy running-config startup-config</th>
</tr>
</thead>
</table>

**Example:**

```
Switch# copy running-config startup-config
```

### What to do next

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).

To remove a specific community string, use the `no snmp-server community-string` global configuration command.

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.
Configuring SNMP Groups and Users

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the switch. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Follow these steps to configure SNMP groups and users on the switch.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **snmp-server engineID**
   
   ```
   local engineid-string | remote ip-address [udp-port port-number]
   ```
4. **snmp-server group**
   
   ```
   group-name {v1 | v2c | v3 {auth | noauth | priv} [read readview] [write writeview] [notify notifyview] [access access-list]}
   ```
5. **snmp-server user**
   
   ```
   username group-name {remote host [udp-port port]} {v1 [access access-list] | v2c [access access-list] | v3 [encrypted] [access access-list] [auth {md5 | sha} auth-password] [priv {des | 3des | aes {128 | 192 | 256}} priv-password]}
   ```
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| **enable** | Enables privileged EXEC mode.
| **Example:** | • Enter your password if prompted.
| Switch> enable | |
| **Step 2**
| **configure terminal** | Enters global configuration mode.
| **Example:** | |
| Switch# configure terminal | |
| **Step 3**
| **snmp-server engineID** | Configures a name for either the local or remote copy of SNMP.
| **Example:** | • The `engineid-string` is a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value. The Step |
### Purpose

Example configures an engine ID of 123400000000000000000000.

- If you select `remote`, specify the `ip-address` of the device that contains the remote copy of SNMP and the optional User Datagram Protocol (UDP) port on the remote device. The default is 162.

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> snmp-server group <strong>group-name</strong> { <strong>v1</strong></td>
<td><strong>v2c</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures a new SNMP group on the remote device. For <code>group-name</code>, specify the name of the group. Specify one of the following security models:</td>
</tr>
<tr>
<td>Switch(config)# snmp-server group public v2c access lmnop</td>
<td><strong>v1</strong> is the least secure of the possible security models.</td>
</tr>
<tr>
<td></td>
<td><strong>v2c</strong> is the second least secure model. It allows transmission of informs and integers twice the normal width.</td>
</tr>
<tr>
<td></td>
<td><strong>v3</strong>, the most secure, requires you to select one of the following authentication levels:</td>
</tr>
<tr>
<td></td>
<td><strong>auth</strong>—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication.</td>
</tr>
<tr>
<td></td>
<td><strong>noauth</strong>—Enables the noAuthNoPriv security level. This is the default if no keyword is specified.</td>
</tr>
<tr>
<td></td>
<td><strong>priv</strong>—Enables Data Encryption Standard (DES) packet encryption (also called privacy).</td>
</tr>
<tr>
<td>(Optional) Enter <strong>read</strong> <strong>readview</strong> with a string (not to exceed 64 characters) that is the name of the view in which you can only view the contents of the agent.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter <strong>write</strong> <strong>writeview</strong> with a string (not to exceed 64 characters) that is the name of the view in which you enter data and configure the contents of the agent.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter <strong>notify</strong> <strong>notifyview</strong> with a string (not to exceed 64 characters) that is the name of the view in which you specify a notify, inform, or trap.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Enter <strong>access</strong> <strong>access-list</strong> with a string (not to exceed 64 characters) that is the name of the access list.</td>
<td></td>
</tr>
</tbody>
</table>

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> snmp-server user <strong>username</strong> <strong>group-name</strong> { <strong>remote</strong> <em>host</em> [ <strong>udp-port</strong> <em>port</em> ] } { <strong>v1</strong> [ <strong>access</strong> | <strong>access-list</strong> ] | | | <strong>v2c</strong> [ <strong>access</strong> | <strong>access-list</strong> ] | | <strong>v3</strong> [ <strong>encrypted</strong> | <strong>access</strong> | <strong>access-list</strong> ] | | <strong>auth</strong> { <strong>md5</strong> | <strong>sha</strong> | <strong>auth-password</strong> } | | <strong>priv</strong> { <strong>des</strong> | <strong>3des</strong> | <strong>aes</strong> { <strong>128</strong> | <strong>192</strong> | <strong>256</strong> } | <strong>priv-password</strong> }</td>
<td>Adds a new user for an SNMP group.</td>
</tr>
<tr>
<td>Example:</td>
<td>The <strong>username</strong> is the name of the user on the host that connects to the agent. The <strong>group-name</strong> is the name of the group to which the user is associated. Enter <strong>remote</strong> to specify a remote SNMP entity to which the user belongs and the hostname or IP address of that</td>
</tr>
<tr>
<td>Switch(config)# snmp-server user Pat public v2c</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring SNMP Groups and Users

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>entity with the optional UDP port number. The default is 162. Enter the SNMP version number (v1, v2c, or v3). If you enter v3, you have these additional options:</td>
</tr>
</tbody>
</table>
| |  • encrypted specifies that the password appears in encrypted format. This keyword is available only when the v3 keyword is specified.  
| |  • auth is an authentication level setting session that can be either the HMAC-MD5-96 (md5) or the HMAC-SHA-96 (sha) authentication level and requires a password string auth-password (not to exceed 64 characters).  
| |  If you enter v3 you can also configure a private (priv) encryption algorithm and password string priv-password using the following keywords (not to exceed 64 characters):  
| |  • priv specifies the User-based Security Model (USM).  
| |  • des specifies the use of the 56-bit DES algorithm.  
| |  • 3des specifies the use of the 168-bit DES algorithm.  
| |  • aes specifies the use of the DES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.  
| |  (Optional) Enter access access-list with a string (not to exceed 64 characters) that is the name of the access list.  
| |  Returns to privileged EXEC mode.  
| |  Verifies your entries.  
| |  (Optional) Saves your entries in the configuration file. |

### Example:

**Step 6**

**Example:**

```
Switch(config)# end
```

**Step 7**

**Example:**

```
Switch# show running-config
```

**Step 8**

**Example:**

```
Switch# copy running-config startup-config
```

**Related Topics**

SNMP Configuration Guidelines, on page 307
Configuring SNMP Notifications

A trap manager is a management station that receives and processes traps. Traps are system alerts that the switch generates when certain events occur. By default, no trap manager is defined, and no traps are sent. Switches running this Cisco IOS release can have an unlimited number of trap managers.

Many commands use the word `traps` in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword `traps` refers to traps, informs, or both. Use the `snmp-server host` global configuration command to specify whether to send SNMP notifications as traps or informs.

You can use the `snmp-server host` global configuration command for a specific host to receive the notification types listed in the following table. You can enable any or all of these traps and configure a trap manager to receive them.

### Table 39: Device Notification Types

<table>
<thead>
<tr>
<th>Notification Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge</td>
<td>Generates STP bridge MIB traps.</td>
</tr>
<tr>
<td>cluster</td>
<td>Generates a trap when the cluster configuration changes.</td>
</tr>
<tr>
<td>config</td>
<td>Generates a trap for SNMP configuration changes.</td>
</tr>
<tr>
<td>copy-config</td>
<td>Generates a trap for SNMP copy configuration changes.</td>
</tr>
<tr>
<td>cpu threshold</td>
<td>Allow CPU-related traps.</td>
</tr>
<tr>
<td>entity</td>
<td>Generates a trap for SNMP entity changes.</td>
</tr>
<tr>
<td>envmon</td>
<td>Generates environmental monitor traps. You can enable any or all of these environmental traps: fan, shutdown, status, supply, temperature.</td>
</tr>
<tr>
<td>errdisable</td>
<td>Generates a trap for a port VLAN errdisabled. You can also set a maximum trap rate per minute. The range is from 0 to 10000; the default is 0, which means there is no rate limit.</td>
</tr>
<tr>
<td>flash</td>
<td>Generates SNMP FLASH notifications. In a switch stack, you can optionally enable notification for flash insertion or removal, which would cause a trap to be issued whenever a switch in the stack is removed or inserted (physical removal, power cycle, or reload).</td>
</tr>
<tr>
<td>fru-ctrl</td>
<td>Generates entity field-replaceable unit (FRU) control traps. In the switch stack, this trap refers to the insertion or removal of a switch in the stack.</td>
</tr>
<tr>
<td>ipmulticast</td>
<td>Generates a trap for IP multicast routing changes.</td>
</tr>
<tr>
<td>mac-notification</td>
<td>Generates a trap for MAC address notifications.</td>
</tr>
<tr>
<td>msdp</td>
<td>Generates a trap for Multicast Source Discovery Protocol (MSDP) changes.</td>
</tr>
<tr>
<td>Notification Type Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ospf</td>
<td>Generates a trap for Open Shortest Path First (OSPF) changes. You can enable any or all of these traps: Cisco specific, errors, link-state advertisement, rate limit, retransmit, and state changes.</td>
</tr>
<tr>
<td>pim</td>
<td>Generates a trap for Protocol-Independent Multicast (PIM) changes. You can enable any or all of these traps: invalid PIM messages, neighbor changes, and rendezvous point (RP)-mapping changes.</td>
</tr>
</tbody>
</table>
| port-security            | Generates SNMP port security traps. You can also set a maximum trap rate per second. The range is from 0 to 1000; the default is 0, which means that there is no rate limit.  

**Note**  When you configure a trap by using the notification type `port-security`, configure the port security trap first, and then configure the port security trap rate:  
1. `snmp-server enable traps port-security`  
2. `snmp-server enable traps port-security trap-rate rate` |
| rtr                      | Generates a trap for the SNMP Response Time Reporter (RTR). |
| snmp                     | Generates a trap for SNMP-type notifications for authentication, cold start, warm start, link up or link down. |
| storm-control            | Generates a trap for SNMP storm-control. You can also set a maximum trap rate per minute. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every occurrence). |
| stpx                     | Generates SNMP STP Extended MIB traps. |
| syslog                   | Generates SNMP syslog traps. |
| tty                      | Generates a trap for TCP connections. This trap is enabled by default. |
| vlan-membership          | Generates a trap for SNMP VLAN membership changes. |
| vlancreate               | Generates SNMP VLAN created traps. |
| vlandelete               | Generates SNMP VLAN deleted traps. |
| vtp                      | Generates a trap for VLAN Trunking Protocol (VTP) changes. |

Follow these steps to configure the switch to send traps or informs to a host.

**SUMMARY STEPS**

1. `enable`  
2. `configure terminal`  
3. `snmp-server engineID remote ip-address engineid-string`  
4. `snmp-server user username group-name { remote host [ udp-port port ] } { v1 [ access access-list ] | v2c [ access access-list ] | v3 [ encrypted ] [ access access-list ] [ auth { md5 | sha } auth-password ] }`  
5. `snmp-server group group-name { v1 | v2c | v3 { auth | noauth | priv } } [ read readview ] [ write writeview ] [ notify notifyview ] [ access access-list ]`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server engineID remote ip-address engine-id-string</td>
<td>Specifies the engine ID for the remote host.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> snmp-server user username group-name { remote host [ udp-port port ] } { v1 [ access access-list ]</td>
<td>v2c [ access access-list ]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# snmp-server user Pat public v2c</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> snmp-server group group-name { v1</td>
<td>v2c</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# snmp-server group public v2c access lmnop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> snmp-server host host-addr [ informs</td>
<td>traps ] [ version { 1</td>
</tr>
</tbody>
</table>

**Note** You cannot configure a remote user for an address without first configuring the engine ID for the remote host. Otherwise, you receive an error message, and the command is not executed.
### Purpose

- **Command or Action**
  - **Example:**
    ```
    Switch(config)# snmp-server host 203.0.113.1 comaccess snmp
    ```

- **Purpose**
  - (Optional) Specify **traps** (the default) to send SNMP traps to the host.
  - (Optional) Specify **informs** to send SNMP informs to the host.
  - (Optional) Specify the SNMP **version** (1, 2c, or 3). SNMPv1 does not support informs.
  - (Optional) For Version 3, select authentication level **auth**, **noauth**, or **priv**.

- **Note**
  - The **priv** keyword is available only when the cryptographic software image is installed.

  - For **community-string**, when **version 1 or version 2c** is specified, enter the password-like community string sent with the notification operation. When **version 3** is specified, enter the SNMPv3 username.

  - The **@** symbol is used for delimiting the context information. Avoid using the **@** symbol as part of the SNMP community string when configuring this command.

  - (Optional) For **notification-type**, use the keywords listed in the table above. If no type is specified, all notifications are sent.

### Step 7

**snmp-server enable traps notification-types**

- **Example:**
  ```
  Switch(config)# snmp-server enable traps snmp
  ```

- **Purpose**
  - Enables the switch to send traps or informs and specifies the type of notifications to be sent. For a list of notification types, see the table above, or enter **snmp-server enable traps ?**.
  
  - To enable multiple types of traps, you must enter a separate **snmp-server enable traps** command for each trap type.

- **Note**
  - When you configure a trap by using the notification type **port-security**, configure the port security trap first, and then configure the port security trap rate:
    1. **snmp-server enable traps port-security**
    2. **snmp-server enable traps port-security trap-rate rate**

### Step 8

**snmp-server trap-source interface-id**

- **Example:**
  ```
  Switch(config)# snmp-server trap-source gigabitethernet 0/1
  ```

- **Purpose**
  - (Optional) Specifies the source interface, which provides the IP address for the trap message. This command also sets the source IP address for informs.

### Step 9

**snmp-server queue-length length**

- **Example:**

- **Purpose**
  - (Optional) Establishes the message queue length for each trap host. The range is 1 to 5000; the default is 10.
What to do next

The `snmp-server host` command specifies which hosts receive the notifications. The `snmp-server enable traps` command globally enables the method for the specified notification (for traps and informs). To enable a host to receive an inform, you must configure an `snmp-server host informs` command for the host and globally enable informs by using the `snmp-server enable traps` command.

To remove the specified host from receiving traps, use the `no snmp-server host host` global configuration command. The `no snmp-server host` command with no keywords disables traps, but not informs, to the host. To disable informs, use the `no snmp-server host informs` global configuration command. To disable a specific trap type, use the `no snmp-server enable traps notification-types` global configuration command.

Related Topics

SNMP Notifications, on page 306
Monitoring SNMP Status, on page 322

Setting the Agent Contact and Location Information

Follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file.

SUMMARY STEPS

1. enable
2. configure terminal
3. `snmp-server contact` text
4. `snmp-server location` text
5. end
6. `show running-config`
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable                       | Enables privileged EXEC mode.  
| Example:                                 | • Enter your password if prompted. |
| Switch> `enable`                         |         |
| **Step 2** `configure terminal`         | Enters global configuration mode. |
| Example:                                 |         |
| Switch# `configure terminal`            |         |
| **Step 3** `snmp-server contact` text   | Sets the system contact string. |
| Example:                                 |         |
| Switch(config)# `snmp-server contact Dial System Operator at beeper 21555` |         |
| **Step 4** `snmp-server location` text  | Sets the system location string. |
| Example:                                 |         |
| Switch(config)# `snmp-server location Building 3/Room 222` |         |
| **Step 5** end                          | Returns to privileged EXEC mode.  |
| Example:                                 |         |
| Switch(config)# `end`                   |         |
| **Step 6** `show running-config`        | Verifies your entries. |
| Example:                                 |         |
| Switch# `show running-config`           |         |
| **Step 7** `copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
| Example:                                 |         |
| Switch# `copy running-config startup-config` |         |
Limiting TFTP Servers Used Through SNMP

Follow these steps to limit the TFTP servers used for saving and loading configuration files through SNMP to the servers specified in an access list.

SUMMARY STEPS

1. enable
2. configure terminal
3. snmp-server tftp-server-list access-list-number
4. access-list access-list-number {deny | permit} source [source-wildcard]
5. end
6. show running-config
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>snmp-server tftp-server-list access-list-number</td>
<td>Limits the TFTP servers used for configuration file copies through SNMP to the servers in the access list.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# snmp-server tftp-server-list 44</td>
<td>For access-list-number, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.</td>
</tr>
<tr>
<td>Step 4</td>
<td>access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# access-list 44 permit 10.1.1.2</td>
<td>For access-list-number, enter the access list number specified in Step 3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For source, enter the IP address of the TFTP servers that can access the switch.</td>
</tr>
</tbody>
</table>
Monitoring SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the `show snmp` privileged EXEC command. You also can use the other privileged EXEC commands listed in the table to display SNMP information.

### Table 40: Commands for Displaying SNMP Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp</td>
<td>Displays SNMP statistics.</td>
</tr>
<tr>
<td>show snmp group</td>
<td>Displays information on the local SNMP engine and all remote engines that have been configured on the device.</td>
</tr>
<tr>
<td>show snmp pending</td>
<td>Displays information on pending SNMP requests.</td>
</tr>
<tr>
<td>show snmp sessions</td>
<td>Displays information on the current SNMP sessions.</td>
</tr>
</tbody>
</table>
**SNMP Examples**

This example shows how to enable all versions of SNMP. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string `public`. This configuration does not cause the switch to send any traps.

```
Switch(config)# snmp-server community public
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string `public`. The switch also sends VTP traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string `public` is sent with the traps.

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the `comaccess` community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host `cisco.com` using the community string `public`.

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host `cisco.com`. The community string is restricted. The first line enables the switch to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous `snmp-server` host commands for the host `cisco.com`.

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```
This example shows how to enable the switch to send all traps to the host `myhost.cisco.com` using the community string `public`:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

This example shows how to associate a user with a remote host and to send `auth` (authNoPriv) authentication-level informs when the user enters global configuration mode:

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Commands</td>
<td><em>Network Management Command Reference, Cisco IOS Release 15.2(2)</em></td>
</tr>
</tbody>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature History and Information for Simple Network Management Protocol

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)E</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 19

Configuring SPAN

• Finding Feature Information, on page 327
• Restrictions for SPAN, on page 327
• Information About SPAN, on page 328
• How to Configure SPAN, on page 329
• Monitoring SPAN Operations, on page 333
• SPAN Configuration Examples, on page 333
• Additional References, on page 334
• Feature History and Information for SPAN, on page 335

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for SPAN

SPAN

The restrictions for SPAN are as follows:

• For SPAN sources, you can monitor traffic for a single port or a series or range of ports for each session.

• The destination port cannot be a source port; a source port cannot be a destination port.

• You cannot have two SPAN sessions using the same destination port.

• When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
• Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the `no monitor session {session_number | all}` global configuration command to delete configured SPAN parameters.

• You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port are enabled.

Traffic monitoring in a SPAN session has the following restrictions:

• The switch supports only one local SPAN session.

• SPAN sessions do not interfere with the normal operation of the switch. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.

• When SPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Monitoring a large number of ports could potentially generate large amounts of network traffic.

• You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port for that session.

Information About SPAN

SPAN

You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports can be monitored by using SPAN.

You can use the SPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

Default SPAN Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPAN state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Source port traffic to monitor</td>
<td>Both received and sent traffic (both).</td>
</tr>
<tr>
<td>Encapsulation type (destination port)</td>
<td>Native form (untagged packets).</td>
</tr>
</tbody>
</table>
Configuration Guidelines

SPAN Configuration Guidelines

- To remove a source or destination port or VLAN from the SPAN session, use the `no monitor session session_number source {interface interface-id | vlan vlan-id}` global configuration command or the `no monitor session session_number destination interface interface-id` global configuration command. For destination interfaces, the `encapsulation` options are ignored with the `no` form of the command.

How to Configure SPAN

Creating a Local SPAN Session

Follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `no monitor session session_number`
4. `monitor session session_number source {interface interface-id} [, -] [both | rx | tx]`
5. `monitor session session_number destination {interface interface-id} [, - ]`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3**
  no monitor session *session_number*  
  Example:  
  Switch(config)# no monitor session 1 | Removes existing SPAN configuration for the specified session. The range is 1 to 4. |
| **Step 4**
  monitor session *session_number* source {interface *interface-id* | [ , ] | *both* | *rx* | *tx*}  
  Example:  
  Switch(config)# monitor session 1 source interface gigabitethernet0/1 | Specifies the SPAN session and the source port (monitored port).  
  • For *session_number*, the range is 1 to 4.  
  • For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (*port-channel* *port-channel-number*). Valid port-channel numbers are 1 to 6.  
  • (Optional) [ , ] | Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.  
  • (Optional) *both* | *rx* | *tx*—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.  
  • *both*—Monitors both received and sent traffic.  
  • *rx*—Monitors received traffic.  
  • *tx*—Monitors sent traffic.  
  **Note** You can use the monitor session *session_number* source command multiple times to configure multiple source ports. |
| **Step 5**
  monitor session *session_number* destination {interface *interface-id* | [ , ] }  
  Example:  
  Switch(config)# monitor session 1 destination interface gigabitethernet0/2 | Specifies the SPAN session and the destination port (monitoring port). The port LED changes to amber when the configuration changes take effect. The LED returns to its original state (green) only after removing the SPAN destination configuration.  
  **Note** For local SPAN, you must use the same session number for the source and destination interfaces.  
  • For *session_number*, specify the session number entered in step 4.  
  • For *interface-id*, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN. |
Creating a Local SPAN Session and Configuring Incoming Traffic

Follow these steps to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

SUMMARY STEPS

1. enable
2. configure terminal
3. no monitor session {session_number | all | local | remote}
4. monitor session session_number source {interface interface-id | vlan vlan-id} [, , -] [both | rx | tx]
5. monitor session session_number destination {interface interface-id [, , -] [encapsulation replicate|ingress {dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id}]}]
6. end
7. show running-config
8. copy running-config startup-config
# Creating a Local SPAN Session and Configuring Incoming Traffic

## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  - enable
  - ```Switch> enable``` | Enables privileged EXEC mode.
  - Enter your password if prompted. |
| **Step 2**
  - configure terminal
  - ```Switch# configure terminal``` | Enters global configuration mode. |
| **Step 3**
  - no monitor session `{session_number | all | local | remote}`
  - ```Switch(config)# no monitor session all``` | Removes any existing SPAN configuration for the session.
  - For `session_number`, the range is 1 to 66.
  - `all`—Removes all SPAN sessions.
  - `local`—Removes all local sessions.
  - `remote`—Removes all remote SPAN sessions. |
| **Step 4**
  - monitor session session_number source `{interface interface-id | vlan vlan-id} [ , | - ] [ both | rx | tx ]`
  - ```Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx``` | Specifies the SPAN session and the source port (monitored port). |
| **Step 5**
  - monitor session session_number destination `{interface interface-id [ , | - ] [ encapsulation replicate | ingress { dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id } ]}`
  - ```Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress dot1q vlan 6``` | Specifies the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation.
  - For `session_number`, specify the session number entered in Step 4.
  - For `interface-id`, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.
  - (Optional) [ , | - ]—Specifies a series or range of interfaces. Enter a space before and after the comma or hyphen.
  - `ingress` enables forwarding of incoming traffic on the destination port and to specify the encapsulation type:
    - `dot1q vlan vlan-id`—Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
    - `untagged vlan vlan-id` or `vlan vlan-id`—Accepts incoming packets with untagged encapsulation.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>type with the specified VLAN as the default VLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring SPAN Operations

The following table describes the command used to display SPAN operations configuration and results to monitor operations:

**Table 42: Monitoring SPAN Operations**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor session</td>
<td>Displays the current SPAN configuration. Enter the <strong>all</strong> keyword to show configuration for all SPAN sessions, the <strong>local</strong> keyword to show configurations for local sessions only, and the <strong>range</strong> keyword to show configurations for a range of SPAN sessions.</td>
</tr>
</tbody>
</table>

### SPAN Configuration Examples

#### Example: Configuring Local SPAN

This example shows how to set up SPAN session 1 for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.
Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
encapsulation replicate
Switch(config)# end

This example shows how to remove port 1 as a SPAN source for SPAN session 1:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet0/1
Switch(config)# end

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 1 source interface gigabitethernet0/1 rx
Switch(config)# end

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination Gigabit Ethernet port 2. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
Switch(config)# end

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on Gigabit Ethernet source port 1, and send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and to enable ingress forwarding with VLAN 6 as the default ingress VLAN:

Switch> enable
Switch# configure terminal
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation replicate ingress vlan 6
Switch(config)# end

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Commands</td>
<td>*Network Management Command Reference, Cisco IOS Release 15.2(2)*E</td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for SPAN

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>Switch Port Analyzer (SPAN): Allows monitoring of switch traffic on a port or VLAN using a sniffer/separator or RMON probe. This feature was introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E Cisco IOS 15.2(5)E</td>
<td>SPAN destination port support on EtherChannels: Provides the ability to configure a SPAN destination port on an EtherChannel. This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E Cisco IOS 15.2(5)E</td>
<td>Switch Port Analyzer (SPAN) - distributed egress SPAN: Provides distributed egress SPAN functionality onto line cards in conjunction with ingress SPAN already been distributed to line cards. By distributing egress SPAN functionalities onto line cards, the performance of the system is improved. This feature was introduced.</td>
</tr>
</tbody>
</table>
PART VI

Network Powered Lighting

- Configuring COAP Proxy Server, on page 339
- Configuring Auto SmartPorts, on page 353
- Configuring 2-event Classification, on page 359
- Configuring Perpetual POE, on page 363
- Frequently Asked Questions, on page 369
CHAPTER 20

Configuring COAP Proxy Server

- Finding Feature Information, on page 339
- Information About the COAP Proxy Server, on page 339
- Restrictions for the COAP Proxy Server, on page 340
- Supported Hardware for the COAP Proxy Server, on page 340
- How to Configure the COAP Proxy Server, on page 342
- Monitoring COAP Proxy Server, on page 346
- Examples: Configuring the COAP Proxy Server, on page 347

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the COAP Proxy Server

The COAP protocol is designed for use with constrained devices. COAP works in the same way on constrained devices as HTTP works on servers in accessing information.

The comparison of COAP and HTTP is shown below:

- In the case of a webserver: HTTP is the protocol; TCP is the transport; and HTML is the most common information format transported.
- In case of a constrained device: COAP is the protocol; UDP is the transport; and JSON/link-format/CBOR is the popular information format.

COAP provides a means to access and control device using a similar GET/POST metaphor and restful API as in HTTP.

Related Topics
- Configuring the COAP Proxy, on page 343
Restrictions for the COAP Proxy Server

The following restrictions apply to COAP proxy server:

- Switch cannot advertise itself as CoAP client using ipv6 broadcast (CSCuw26467).
- Support for Observe Not Implemented.
- Blockwise requests are not supported. We handle block-wise responses and can generate block-wise responses.
- DTLS Support is for the following modes only RawPublicKey and Certificate Based.
- IPv6 DTLS is not supported on the 3850 Platform.
- Switch does not act as DTLS client. DTLS for endpoints only.
- Endpoints are expected to handle and respond with CBOR payloads.
- Client side requests are expected to be in JSON.
- Switch cannot advertise itself to other Resource Directories as IPv6, due to an IPv6 broadcast issue.
- Configuration of Fast PoE, Perpetual PoE or 2-event classification has to be done before physically connecting any endpoint. Alternatively do a manual shut/no-shut of the ports drawing power.
- Power to the ports will be interrupted in case of MCU firmware upgrade and ports will be back up immediately after the upgrade.

Supported Hardware for the COAP Proxy Server

COAP Proxy Server is supported on the following Catalyst 3850 Switch Models:

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Cisco IOS Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C3850-24T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>Switch Model</td>
<td>Cisco IOS Image</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WS-C3850-24U-S</td>
<td>IP Base</td>
<td>Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>WS-C3850-48U-S</td>
<td>IP Base</td>
<td>Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply</td>
</tr>
<tr>
<td>WS-C3850-12S-S</td>
<td>IP Base</td>
<td>Stackable 12 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-S</td>
<td>IP Base</td>
<td>Stackable 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply</td>
</tr>
<tr>
<td>WS-C3850-16XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-24XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-32XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-48XS-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WSC850-48XS-F-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24XU-S</td>
<td>IP Base</td>
<td>Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set</td>
</tr>
</tbody>
</table>
### How to Configure the COAP Proxy Server

To configure the COAP proxy server, you can configure the COAP Proxy and COAP Endpoints in the Configuration mode.

The commands are: `coap [proxy | endpoints].`

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Cisco IOS Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C3850-48F-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set</td>
</tr>
<tr>
<td>WS-3850-24U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply</td>
</tr>
<tr>
<td>WS-3850-48U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12S-E</td>
<td>IP Services</td>
<td>Stackable, 2 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-E</td>
<td>IP Services</td>
<td>Stackable, 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-16XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-32XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-48XS-E</td>
<td>IP Services</td>
<td>Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WSC850-48XS-E</td>
<td>IP Services</td>
<td>Stackable, SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24XU-E</td>
<td>IP Services</td>
<td>Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
</tbody>
</table>
Configuring the COAP Proxy

To start or stop the COAP proxy on the switch, perform the steps given below:

SUMMARY STEPS

1. enable
2. configure terminal
3. coap proxy
4. security [none | [ipv4 | ipv6] {ip-address ip-mask/prefix} | list {ipv4-list name | ipv6-list-name}] | dtls [id-trustpoint {identity-trustpoint label}] | [verification-trustpoint {verification-trustpoint} | [ipv4 | ipv6 {ip-address ip-mask/prefix}] | list {ipv4-list name | ipv6-list-name}]
5. max-endpoints {number}
6. port-unsecure {port-num}
7. port-dtls {port-num}
8. resource-directory [ipv4 | ipv6] {ip-address}
9. list [ipv4 | ipv6] {list-name}
10. start
11. stop
12. exit
13. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong> Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong> Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>coap proxy</strong> Enters the COAP proxy sub mode.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# coap proxy</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>security</strong> [none</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• none - Indicates no security on that port. With security none, a maximum of 5 ipv4 and 5 ipv6 addresses can be associated.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Example:</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config-coap-proxy)# security none ipv4 1.1.0.0 255.255.0.0 | - dtls - The DTLS security takes RSA trustpoint and Verification trustpoint which are optional. Without Verification trustpoint it does the normal Public Key Exchange.

With security dtls, a maximum of 5 ipv4 and 5 ipv6 addresses can be associated. |

**Note** To delete all security configurations under coap proxy, use the *no security* command. |

### Step 5

<table>
<thead>
<tr>
<th>max-endpoints {number}</th>
<th>(Optional) Specifies the maximum number of endpoints that can be learnt on the switch. The default value is 10. The range is 1 to 500.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-coap-proxy)#max-endpoints 10</td>
<td>To delete all max-endpoints configured under coap proxy, use the <em>no max-endpoints</em> command.</td>
</tr>
</tbody>
</table>

### Step 6

<table>
<thead>
<tr>
<th>port-unsecure {port-num}</th>
<th>(Optional) Configures a port other than the default 5683. The range is 1 to 65000.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-coap-proxy)#port-unsecure 5683</td>
<td>To delete all port configurations under coap proxy, use the <em>no port-unsecure</em> command.</td>
</tr>
</tbody>
</table>

### Step 7

<table>
<thead>
<tr>
<th>port-dtls {port-num}</th>
<th>(Optional) Configures a port other than the default 5684.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-coap-proxy)#port-dtls 5864</td>
<td>To delete all dtls port configurations under coap proxy, use the <em>no port-dtls</em> command.</td>
</tr>
</tbody>
</table>

### Step 8

| resource-directory [ipv4 | ipv6] {ip-address} | Configures a unicast upstream resource directory server to which the switch can act as a COAP client. |
|-----------------------|---------------------------------------------------------|
| Example:              |                                                         |
| Switch(config-coap-proxy)#resource-directory ipv4 192.168.1.1 | With resource-directory, a maximum of 5 of ipv4 and 5 ipv6, ip addresses can be configured. |

**Note** To delete all resource directory configurations under coap proxy, use the *no resource-directory* command. |

### Step 9

<p>| list [ipv4 | ipv6] {list-name} | (Optional) Restricts the IP address range where the lights and their resources can be learnt. Creates a named list of ip address/masks, to be used in the <em>security</em> command options above. |
|---------------------|---------------------------------------------------------|
| Example:            |                                                         |
| Switch(config-coap-proxy)#list ipv4 trial_list | With list, a maximum of 5 ip-lists can be configured, irrespective of ipv4 or ipv6. We can configure a max of 5 ip addresses per ip-list. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>start</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Starts the COAP proxy on this switch.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td><strong>stop</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Stops the COAP proxy on this switch.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Exits the COAP proxy sub mode.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 13</td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Information About the COAP Proxy Server](#), on page 339
- [Examples: Configuring the COAP Proxy Server](#), on page 347

### Configuring COAP Endpoints

To configure the COAP Proxy to support multiple IPv4/IPv6 static-endpoints, perform the steps given below:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. coap endpoint [ ipv4 | ipv6 ] {ip-address}
4. exit
5. end
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> coap endpoint [ipv4</td>
<td>ipv6] {ip-address}</td>
</tr>
<tr>
<td>Example:</td>
<td>• ipv4 - Configures the IPv4 Static endpoints.</td>
</tr>
<tr>
<td>Switch(config)# coap endpoint ipv4 1.1.1.1</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# coap endpoint ipv6 2001::1</td>
<td>• ipv6 - Configures the IPv6 Static endpoints.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To stop the coap proxy on any endpoint, use the no coap endpoint [ipv4</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits the COAP endpoint sub mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-coap-endpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Monitoring COAP Proxy Server

To display the COAP protocol details, use the commands in the following table:

Table 43: Commands to Display to COAP specific data

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show coap version</td>
<td>Shows the IOS COAP version and the RFC information.</td>
</tr>
<tr>
<td>show coap resources</td>
<td>Shows the resources of the switch and those learnt by it.</td>
</tr>
<tr>
<td>show coap endpoints</td>
<td>Shows the endpoints which are discovered and learnt.</td>
</tr>
</tbody>
</table>
### Examples: Configuring the COAP Proxy Server

This example shows how you can configure the port number 5683 to support a maximum of 10 endpoints.

```
Switch#coap proxy security none ipv4 2.2.2.2 255.255.255.0 port 5683 max-endpoints 10
```

This example shows how to configure COAP proxy on ipv4 1.1.0.0 255.255.0.0 with no security settings.

```
Switch(config-coap-proxy)# security
  dtls  dtls
  none  no security

Switch(config-coap-proxy)#security none
  ipv4  IP address range on which to learn lights
  ipv6  IPv6 address range on which to learn lights
  list  IP address range on which to learn lights

Switch(config-coap-proxy)#security none ipv4
  A.B.C.D {/nn || A.B.C.D} IP address range on which to learn lights
```

---

### Table 44: Commands to Clear COAP Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear coap database</td>
<td>Clears the COAP learnt on the switch, and the internal database of endpoint information.</td>
</tr>
</tbody>
</table>

To debug the COAP protocol, use the commands in the following table:

### Table 45: Commands to Debug COAP protocol

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug coap database</td>
<td>Debugs the COAP database output.</td>
</tr>
<tr>
<td>debug coap errors</td>
<td>Debugs the COAP errors output.</td>
</tr>
<tr>
<td>debug coap events</td>
<td>Debugs the COAP events output.</td>
</tr>
<tr>
<td>debug coap packets</td>
<td>Debugs the COAP packets output.</td>
</tr>
<tr>
<td>debug coap trace</td>
<td>Debugs the COAP traces output.</td>
</tr>
<tr>
<td>debug coap warnings</td>
<td>Debugs the COAP warnings output.</td>
</tr>
<tr>
<td>debug coap all</td>
<td>Debugs all the COAP output.</td>
</tr>
</tbody>
</table>

---

**Note**

If you wish to disable the debugs, prepend the command with a "no" keyword.
Switch(config-coap-proxy)#security none ipv4 1.1.0.0 255.255.0.0

This example shows how to configure COAP proxy on *ipv4 1.1.0.0 255.255.0.0* with **dtls id trustpoint** security settings.

Switch(config-coap-proxy)#security dtls?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Switch(config-coap-proxy)#security dtls id-trustpoint?
   WORD  Identity TrustPoint Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT?
  verification-trustpoint Certificate Verification Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT

Switch(config-coap-proxy)#security dtls?
  id-trustpoint DTLS RSA and X.509 Trustpoint Labels
  ipv4 IP address range on which to learn lights
  ipv6 IPv6 address range on which to learn lights
  list IP address range on which to learn lights

Switch(config-coap-proxy)# security dtls ipv4 1.1.0.0 255.255.0.0

---

**Note**

For configuring *ipv4 / ipv6 / list*, the **id-trustpoint** and (optional) **verification-trustpoint**, should be pre-configured, else the system shows an error.

Switch(config-coap-proxy)#security dtls ipv4 1.1.0.0 255.255.0.0

---

This example shows how to configure a Trustpoint. This is a pre-requisite for COAP security **dtls** with **id trustpoint** configurations.

**ip domain-name myDomain**

crypto key generate rsa general-keys exportable label MyLabel modulus 2048

Switch(config)#crypto pki trustpoint MY_TRUSTPOINT
Switch(config)#crypto pki rsakeypair MyLabel 2048
Switch(config)#crypto pki enrollment selfsigned
Switch(config)#crypto pki exit

Switch(config)#crypto pki enroll MY_TRUSTPOINT
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

---

This example shows how to configure COAP proxy on *ipv4 1.1.0.0 255.255.0.0* with **dtls verification trustpoint** (DTLS with certificates or verification trustpoints)
Switch(config-coap-proxy)#security dtls ?
    id-trustpoint DTLS RSA and X.509 Trustpoint Labels
    ipv4 IP address range on which to learn lights
    ipv6 IPv6 address range on which to learn lights
    list IP address range on which to learn lights

Switch(config-coap-proxy)#security dtls id-trustpoint ?
    WORD Identity TrustPoint Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT ?
    verification-trustpoint Certificate Verification Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT verification-trustpoint
    WORD Identity TrustPoint Label

Switch(config-coap-proxy)#security dtls id-trustpoint RSA-TRUSTPOINT verification-trustpoint
    CA-TRUSTPOINT ?

-----------------------------------------------------------------------------------------------

This example shows how to configure Verification Trustpoint. This is a pre-requisite for COAP security dtls with verification trustpoint configurations.

Switch(config)#crypto pki import CA-TRUSTPOINT pkcs12 flash:hostA.p12 password cisco123
% Importing pkcs12...
Source filename [hostA.p12]?
Reading file from flash:hostA.p12
CRYPTO_PKI: Imported PKCS12 file successfully.

-----------------------------------------------------------------------------------------------

This example shows how to create a list named trial-list, to be used in the security [ none | dtls ] command options.

Switch(config-coap-proxy)#list ipv4 trial_list
Switch (config-coap-proxy-iplist)#1.1.0.0 255.255.255.0
Switch (config-coap-proxy-iplist)#2.2.0.0 255.255.255.0
Switch (config-coap-proxy-iplist)#3.3.0.0 255.255.255.0
Switch (config-coap-proxy-iplist)#exit
Switch (config-coap-proxy)#security none list trial_list

-----------------------------------------------------------------------------------------------

This example shows all the negation commands available in the coap-proxy sub mode.

Switch(config-coap-proxy)#no ?
    ip-list Configure IP-List
    max-endpoints maximum number of endpoints supported
    port-unsecure Specify a port number to use
    port-dtls Specify a dtls-port number to use
    resource-discovery Resource Discovery Server
    security CoAP Security features

-----------------------------------------------------------------------------------------------

This example shows how you can configure multiple IPv4/IPv6 static-endpoints on the coap proxy.
Switch (config)# coap endpoint ipv4 1.1.1.1
Switch (config)# coap endpoint ipv4 2.1.1.1
Switch (config)# coap endpoint ipv6 2001::1

This example shows how you can display the COAP protocol details.

Switch# show coap version
CoAP version 1.0.0
RFC 7252

Switch# show coap resources
Link format data =
</> </1.1.1.6/cisco/context>
</1.1.1.6/cisco/actuator>
</1.1.1.6/cisco/sensor>
</1.1.1.6/cisco/lldp>
</1.1.1.5/cisco/context>
</1.1.1.5/cisco/actuator>
</1.1.1.5/cisco/sensor>
</1.1.1.5/cisco/lldp>
</cisco/flood>
</cisco/context>
</cisco/showtech>
</cisco/lldp>

Switch# show coap globals
Coap System Timer Values :
Discovery : 120 sec
Cache Exp : 5 sec
Keep Alive : 120 sec
Client DB : 60 sec
Query Queue : 500 ms
Ack delay : 500 ms
Timeout : 5 sec
Max Endpoints : 10
Resource Disc Mode : POST

Switch# show coap stats
Coap Stats :
Endpoints : 2
Requests : 20
Ext Queries : 0

Switch# show coap endpoints
List of all endpoints :

Code : D - Discovered, N - New
# Status Age(s) LastWK(s) IP
-----------------------------------------------
1 D 10 94 1.1.1.6
2 D 6 34 1.1.1.5

Endpoints - Total : 2 Discovered : 2 New : 0
This example shows all options available to debug the COAP protocol.

This example shows all options available to debug the COAP protocol.

Related Topics

- Configuring the COAP Proxy, on page 343
- Information About the COAP Proxy Server, on page 339
Examples: Configuring the COAP Proxy Server
Configuring Auto SmartPorts

- Finding Feature Information, on page 353
- Information about Auto SmartPorts, on page 353
- Auto SmartPort Macros, on page 354
- Commands executed by CISCO_LIGHT_AUTO_SMARTPORT, on page 354
- Enabling Auto SmartPort, on page 355
- Configuring Mapping Between Event Triggers and Built-in Macros, on page 356
- Example: Enabling Auto SmartPorts, on page 358
- Example: Configuring Mapping Between Event Triggers and Built-in Macros, on page 358

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information about Auto SmartPorts

Auto SmartPort macros dynamically configure ports based on the device type detected on the port. When the switch detects a new device on a port, it applies the appropriate Auto SmartPorts macro. When a link-down event occurs on the port, the switch removes the macro. For example, when you connect a Cisco IP phone to a port, Auto SmartPorts automatically applies the Cisco IP phone macro. The Cisco IP phone macro enables quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper treatment of delay-sensitive voice traffic.

Auto SmartPorts uses event triggers to map devices to macros. The most common event triggers are based on Cisco Discovery Protocol (CDP) messages received from connected devices. The detection of a device (Cisco IP phone, Cisco wireless access point, or Cisco router) invokes an event trigger for that device.
Although Auto SmartPort detects the Cisco switch it does not invoke the event trigger automatically. The event trigger needs to be manually invoked to map the switch to macros.

Note

Link Layer Discovery Protocol (LLDP) is used to detect devices that do not support CDP. Other mechanisms used as event triggers include the 802.1X authentication result and MAC-address learned.

System built-in event triggers exist for various devices based mostly on CDP and LLDP messages and some MAC address. These triggers are enabled as long as Auto SmartPort is enabled.

You can configure user-defined trigger groups for profiles and devices. The name of the trigger group is used to associate a user-defined macro.

Auto SmartPort Macros

The Auto SmartPort macros are groups of CLI commands. Detection of devices on a port triggers the application of the macro for the device. System built-in macros exist for various devices, and, by default, system built-in triggers are mapped to the corresponding built-in macros. You can change the mapping of built-in triggers or macros as needed.

A macro basically applies or removes a set of CLIs on an interface based on the link status. In a macro, the link status is checked. If the link is up, then a set of CLIs is applied; if the link is down, the set is removed (the no format of the CLIs are applied). The part of the macro that applies the set of CLIs is termed macro. The part that removes the CLIs (the no format of the CLIs) are termed antimacro.

When a device is connected to an Auto SmartPort, if it gets classified as a lighting end point, it invokes the event trigger `CISCO_LIGHT_EVENT`, and the macro `CISCO_LIGHT_AUTO_SMARTPORT` is executed.

Related Topics

- Enabling Auto SmartPort, on page 355
- Example: Enabling Auto SmartPorts, on page 358

Commands executed by `CISCO_LIGHT_AUTO_SMARTPORT`

When the macro is executed, it runs a series of commands on the switch.

The commands that are executed by running the macro `CISCO_LIGHT_AUTO_SMARTPORT` are:

- `switchport mode access`
- `switchport port-security violation restrict`
- `switchport port-security mac-address sticky`
- `switchport port-security`
- `power inline port poe-ha`
- `storm-control broadcast level 50.00`
- `storm-control multicast level 50.00`
- `storm-control unicast level 50.00`
Enabling Auto SmartPort

Note
Auto SmartPort is disabled by default.

To disable Auto SmartPorts macros on a specific port, use the no macro auto global processing interface command before enabling Auto SmartPort globally.

To enable Auto SmartPort globally, use the macro auto global processing global configuration command.

To enable Auto SmartPorts, perform this task:

SUMMARY STEPS
1. enable
2. configure terminal
3. device classifier
4. macro auto global processing
5. end
6. show running-config
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 device classifier</td>
<td>Enables the device classifier.</td>
</tr>
<tr>
<td>Example: Switch(config)# device classifier</td>
<td>Use no device classifier command to disable the device classifier.</td>
</tr>
<tr>
<td>Step 4 macro auto global processing</td>
<td>Enables Auto SmartPorts on the switch globally.</td>
</tr>
</tbody>
</table>
### Configuring Mapping Between Event Triggers and Built-in Macros

**Purpose**

Use `no macro auto global processing` command to disable Auto SmartPort globally.

**Step 5**

```
Switch(config)# end
```

Returns to privileged EXEC mode.

**Step 6**

```
Switch# show running-config
```

Verifies your entries.

**Step 7**

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

---

**Related Topics**

- Auto SmartPort Macros, on page 354
- Example: Enabling Auto SmartPorts, on page 358

---

**Configuring Mapping Between Event Triggers and Built-in Macros**

**Note**

You need to perform this task when a Cisco switch is connected to the Auto SmartPort.

To map an event trigger to a built-in macros, perform this task:

**Before you begin**

You need to enable auto smartport macros globally.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `macro auto execute event trigger builtin built-in macro name`
4. `macro auto trigger event trigger`
5. `device device_ID`
6. `end`
7. `show shell triggers`
8. `show running-config`
9. `copy running-config startup-config`

## Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>macro auto execute event trigger builtin built-in macro name</code></td>
<td>Specifies a user-defined event trigger and a macro name. This action configures mapping from an event trigger to a built-in Auto Smartports macro.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>macro auto trigger event trigger</code></td>
<td>Invokes the user-defined event trigger.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>macro auto trigger CISCO_SWITCH_EVENT</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>device device_ID</code></td>
<td>Matches the event trigger to the device identifier.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>device cisco WS-C3560CX-8PT-S</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show shell triggers</code></td>
<td>Displays the event triggers on the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>show shell triggers</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>show running-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Example: Enabling Auto SmartPorts

This example shows how you can enable Auto SmartPort.

```
Switch> enable
Switch# configure terminal
Switch(config)# device classifier
Switch(config)# macro auto global processing
Switch(config)# end
```

Related Topics
- Enabling Auto SmartPort, on page 355
- Auto SmartPort Macros, on page 354

Example: Configuring Mapping Between Event Triggers and Built-in Macros

This example shows how you can configure mapping between event triggers and built-in macros.

```
Switch> enable
Switch# configure terminal
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
Switch(config)# macro auto trigger CISCO_SWITCH_EVENT
Switch(config)# device cisco WS-C3560CX-8PT-S
Switch(config)# end
```
CHAPTER 22

Configuring 2-event Classification

- Finding Feature Information, on page 359
- Information about 2-event Classification, on page 359
- Configuring 2-event Classification, on page 359
- Example: Configuring 2-Event Classification, on page 360

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

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:
SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. power inline port 2-event
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Specifies the physical port to be configured, and enters</td>
</tr>
<tr>
<td>Example:</td>
<td>interface configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4 power inline port 2-event</td>
<td>Configures 2-event classification on the switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# power inline port 2-event</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
Example: Configuring 2-Event Classification, on page 360

Example: Configuring 2-Event Classification

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

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

Related Topics

Configuring 2-event Classification, on page 359
Configuring Perpetual POE

- Finding Feature Information, on page 363
- Perpetual POE, on page 363
- Fast POE, on page 363
- Supported Hardware for Perpetual POE, Fast POE and 2-event, on page 364
- Configuring Fast POE, on page 366
- Example: Configuring Perpetual POE, on page 367

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Perpetual POE

The Perpetual POE provides uninterrupted power to connected PD device even when the PSE switch is booting.

\[\text{Note}\]

Power to the ports will be interrupted in case of MCU firmware upgrade and ports will be back up immediately after the upgrade.

Fast POE

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 command `poe-ha`. 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.

## Supported Hardware for Perpetual POE, Fast POE and 2-event

Perpetual POE is supported on the following Catalyst 3850 Switch Models:

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Cisco IOS Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C3850-24T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48T-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48P-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-48F-S</td>
<td>IP Base</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Base feature set</td>
</tr>
<tr>
<td>WS-C3850-24U-S</td>
<td>IP Base</td>
<td>Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100W power supply</td>
</tr>
<tr>
<td>WS-C3850-48U-S</td>
<td>IP Base</td>
<td>Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100W power supply</td>
</tr>
<tr>
<td>WS-C3850-12S-S</td>
<td>IP Base</td>
<td>Stackable 12 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-24S-S</td>
<td>IP Base</td>
<td>Stackable 24 SFP module slots, 1 network module slot, 350-W power supply</td>
</tr>
<tr>
<td>WS-C3850-12XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply</td>
</tr>
<tr>
<td>WS-C3850-16XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-24XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.</td>
</tr>
<tr>
<td>Switch Model</td>
<td>Cisco IOS Image</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WS-C3850-32XS-S</td>
<td>IP Base</td>
<td>Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-S switch.</td>
</tr>
<tr>
<td>WS-C3850-48XS-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-48XS-F-S</td>
<td>IP Base</td>
<td>Stackable, with SFP+ transceivers, 48 ports that support up to 10 G, and 4 ports that support up to 40 G. 750 W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24XS-S</td>
<td>IP Base</td>
<td>Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set.</td>
</tr>
<tr>
<td>WS-C3850-48T-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set.</td>
</tr>
<tr>
<td>WS-C3850-24P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set.</td>
</tr>
<tr>
<td>WS-C3850-48P-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set.</td>
</tr>
<tr>
<td>WS-C3850-48F-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set.</td>
</tr>
<tr>
<td>WS-3850-24U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
<tr>
<td>WS-3850-48U-E</td>
<td>IP Services</td>
<td>Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-12S-E</td>
<td>IP Services</td>
<td>Stackable, 2 SFP module slots, 1 network module slot, 350-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-24S-E</td>
<td>IP Services</td>
<td>Stackable, 24 SFP module slots, 1 network module slot, 350-W power supply.</td>
</tr>
<tr>
<td>WS-C3850-12XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 -W power supply.</td>
</tr>
<tr>
<td>WS-C3850-16XS-E</td>
<td>IP Services</td>
<td>Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-E switch.</td>
</tr>
</tbody>
</table>
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`.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `power inline port poe-ha`
5. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

interface interface-id

*Example:*

Switch(config)# interface gigabitethernet2/0/1

**Purpose:** Specifies the physical port to be configured, and enters interface configuration mode.

**Step 4**

power inline port poe-ha

*Example:*

Switch(config-if)# power inline port poe-ha

**Purpose:** Configures POE High Availability.

**Step 5**

de

*Example:*

Switch(config-if)# end

**Purpose:** Returns to privileged EXEC mode.

---

**Related Topics**

[Example: Configuring Perpetual POE](#), on page 367

---

**Example: Configuring Perpetual POE**

This example shows how you can configure perpetual POE on the switch.

Switch> enable
Switch# configure terminal
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# power inline port poe-ha
Switch(config-if)# end

**Related Topics**

[Configuring Fast POE](#), on page 366
Example: Configuring Perpetual POE
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Frequently Asked Questions

This section lists some frequently asked questions about Network Powered Lighting.

• Question:
  What does "New Endpoint" in the "show coap stats" output mean? When does "New Endpoint" migrate to "Endpoint"?

  Answer:
  New endpoint means that an endpoint has been seen (Discovery packets received) but not yet registered by the CoAP proxy. The CoAP proxy will periodically look at the new endpoint and then send them a GET on “/well-known/core” to get more details, and once RSP is received, it is moved to “Endpoint”.

• Question:
  Why can I not do a "CoAP start" unless there is a security configuration?

  Answer:
  We need to ensure that all configurations related to CoAP are done and then it can be explicitly enabled. This avoids any intermittent unstable states across configurations.

• Question:
Why do we need to enforce drop into the “coap proxy” configuration mode “coap proxy <cr>”? When I have completed the configuration, I have to exit twice to get back to the switch prompt. I do not find this very user friendly.

**Answer:**

We would alternatively have to type “coap proxy” as prefix for each configuration that we do. It is a better option to get into a sub-mode, as all the configurations under the sub-mode relating to coap-proxy can be done.

**Question:**

Why am I not able to unconfigure security or other parameters without first stopping the coap process?

**Answer:**

We need to ensure that all configurations related to CoAP are done and then it can be explicitly enabled. This also avoids and controls the complexity where the user might configure settings on the fly, when CoAP is enabled.

**Question:**

When I stop coap, all configurations associated with the CoAP process are not removed automatically (or return to defaults). Why does the CoAP remember previous configuration? This seems very hard for users to start fresh.

**Answer:**

The system has been intentionally designed this way and this is expected behavior. Sometimes we just want to make minor changes, like change max-endpoints and re-start the proxy. It is a better option to hold all other configurations in place, else the user has to configure everything all over again.

**Question:**

How can I see what the security configurations have been set?

**Answer:**

The command “show run” shows all the configurations.

**Question:**

How can I tune the timer values?

**Example:**

```
wtssa-3850#sho coap glo
Coap System Timer Values:
  Discovery : 120 sec
  Cache Exp : 5 sec
  Keep Alive : 120 sec
  Client DB : 5 sec
  Query Queue : 500 ms
  Ack delay : 500 ms
  Timeout : 5 sec
  Max Endpoints : 500
  Resource Disc Mode : POST
```

**Answer:**

The timer values are fixed and are not tunable at the moment. The reason for this is to avoid inconsistency across systems.
• **Question:**
  What are the commands “list” and “endpoint” used for?

**Answer:**
The “list” command is to make it easier to configure multiple ip-addresses and give a name to it. Then you can assign the name instead of a single ip, to represent multiple ip’s. The "endpoint" command is used to configure a static end point, in cases where the endpoints do not advertise themselves.

• **Question:**
  How can I find the endpoint-to-port mapping by using the “show” command?

**Answer:**
We do not support that of now. However, other commands can be run to fetch this data. Currently, we can still get all the details mentioned using individual commands like “lldp neighbours”, “ip dhcp”, “power inlines” and so on.
PART VII

Configuring EnergyWise

• Configuring EnergyWise, on page 375
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring EnergyWise

Prerequisites for Wake on LAN

- Check that you have enabled Wake on LAN (WoL) in the BIOS and the NIC of the PC that you want to wake up. Refer to your PC documentation for instructions on how to enable WoL in the BIOS and the NIC.
- WoL packets are sent as Layer 2 broadcast packets. To prevent broadcast storms, remove loops by using the Spanning Tree Protocol (STP).
• Check that an EnergyWise WoL query always has a name or keyword attribute associated with it. The importance, name, and keyword fields in the WoL query packet refer to attributes set on the interface that the PC connects to. WoL packets are sent only from interfaces where the name or keyword attribute is set, which prevents broadcast storms. For example, enter this command:

```plaintext
DomainMember# configure terminal
DomainMember(config)# interface gigabitethernet 0/1
DomainMember(config-if)# energywise name PC-1
DomainMember(config-if)# end
DomainMember(config)# end
DomainMember#
DomainMember# energywise query importance 100 name PC-1 wol mac <mac-address>
```

Related Topics

- Using WoL with a MAC Address, on page 401
- Using WoL Without a MAC Address, on page 402
- Wake on LAN, on page 384

## Restrictions for Configuring EnergyWise

### Voice over IP and the Emergency Calling Services

**Warning**

Voice over IP (VoIP) service and the emergency calling service do not function if power fails or is disrupted. After power is restored, you might have to reset or reconfigure equipment to regain access to VoIP and the emergency calling service. In the USA, this emergency number is 911. You need to be aware of the emergency number in your country. Statement 361.

For more information, see the "Important Notice" appendix.

## Information About Configuring EnergyWise

### Cisco EnergyWise Network

In a network, Cisco EnergyWise monitors and manages the power usage of network devices and devices connected to the network.
**EnergyWise Domain**

A Cisco EnergyWise domain is considered to be one unit of power management. The domain consists of Cisco networking devices, Power over Ethernet (PoE) endpoints, and endpoints running agents that are built using the software development kit (SDK) library. This domain is similar to a network-management community such as a VLAN Trunking Protocol (VTP) domain.

For example, if you have a building with a core router, 10 access switches, and 400 endpoints, such as phones, access points, and PCs, you can create an EnergyWise domain called MyBuilding with the router and switches as domain members.
If you want to implement power management applications on a management station and endpoints, all the domain members must run Cisco EnergyWise Version 2.6 or later.

After you enable and configure EnergyWise on the core router and access switches, the MyBuilding domain configures itself. Neighbor relationships are set among the domain members.

• Domain members use CDP when it is enabled or EnergyWise UDP messages to automatically discover neighbors.

• You can manually configure static neighbors.

Each domain member sets up a parent-child relationship with an attached endpoint. For example, an IP phone (child) is connected to a PoE switch (parent), or a PC (child) is connected to a router (parent).

After the domain is set, a domain member can forward queries and control messages to other domain members and endpoints. You can do the following:

• Use SNMP or a management station to query every domain member or endpoint.

• Use the domain member CLI to run an EnergyWise query to receive or set power usage information.

• Use a management application, server, or domain member CLI to define power usage policies or receive power usage information.

Related Topics
Configuring Domain Member or Endpoint Attributes, on page 388
Examples: Setting the Domain, on page 406

Power Level Energy Management

Cisco EnergyWise uses a set of power levels to consistently manage power usage. A power level is a measure of the energy consumed by devices in an EnergyWise network.

The range is from 0 to 10. The default is 10.

Table 46: Power Levels

<table>
<thead>
<tr>
<th>Category</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>10</td>
<td>Full</td>
</tr>
<tr>
<td>Operational</td>
<td>9</td>
<td>High</td>
</tr>
<tr>
<td>Operational</td>
<td>8</td>
<td>Reduced</td>
</tr>
<tr>
<td>Standby</td>
<td>7</td>
<td>Medium</td>
</tr>
<tr>
<td>Standby</td>
<td>6</td>
<td>Frugal</td>
</tr>
<tr>
<td>Standby</td>
<td>5</td>
<td>Low</td>
</tr>
<tr>
<td>Standby</td>
<td>4</td>
<td>Ready</td>
</tr>
<tr>
<td>Standby</td>
<td>3</td>
<td>Standby</td>
</tr>
<tr>
<td>Nonoperational</td>
<td>2</td>
<td>Sleep</td>
</tr>
</tbody>
</table>
The devices in an EnergyWise network can be from different manufacturers.

A Cisco switch does not support level 0. You cannot turn off the power on a switch.

A PoE endpoint, such as an IP phone, receives power from a PoE switch port. The following are the PoE endpoint power characteristics:

- The power level applies to the port.
- The port supports levels 0 to 10.
- If the port power level is 0, the port does not provide power to connected endpoints.
- If the power level is between 1 and 10, the port is operational.

### Attributes

The following table describes Cisco EnergyWise attributes.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Definition</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importance</td>
<td>Device rating based on the business or deployment context.</td>
<td>The range is from 1 (least important) to 100 (most important). The default is 1.</td>
</tr>
<tr>
<td>Keywords</td>
<td>Device description (other than the name or role) for which query results are filtered.</td>
<td>None.</td>
</tr>
<tr>
<td>Name</td>
<td>Device identity for which query results are filtered.</td>
<td>For a PoE port, the short version of the port name. For example, Gi0.2 for Gigabit Ethernet 0/2. For a domain member, the hostname. For an endpoint, see the endpoint documentation. We recommend that you use the hostname.</td>
</tr>
<tr>
<td>Role</td>
<td>Device function based on the business or deployment context.</td>
<td>For a PoE port, the default is interface. For a domain member, the default can be the model number or the supervisor model number. For an endpoint, see the endpoint documentation.</td>
</tr>
</tbody>
</table>
Security

A Cisco EnergyWise network has three levels of security to prevent unauthorized communication.

- The management secret authenticates communication between the domain members and the management station.
- The domain secret authenticates communication between domain members.
- The endpoint secret authenticates communication between domain members and endpoints.

The network enforces security with shared secrets, also referred to as passwords.

Recurrences

A recurrence is an event that repeats on a regular schedule. You can use this feature to schedule jobs to run periodically or at certain times or date. For example, you can configure the domain member to power an endpoint or interface on and off based on the time or date.

A recurrence uses the domain member time.

When configuring recurrences, you specify the time in CRON format (24-hour format). Cron is the time-based job scheduler in Unix computer operating systems.
When a recurrence occurs, changes to the Cisco EnergyWise power level exist only in the running configuration and are not saved in the startup configuration. If the domain member fails and then restarts, it uses the power level in the saved startup configuration.

Related Topics
Configuring Recurrences, on page 394

Time Format and Time Zone
For time format, use the 24-hour clock. The time zone is based on the domain member.

• To set a recurrence at a specific time, enter the `energywise level level recurrence importance importance at minute hour day_of_month month day_of_week` interface configuration command.

For example, to configure a recurrence that occurs every day at 06:34, enter the `energywise level level recurrence importance at 34 6 * * *` command.

• `minute` is 34.
• `hour` is 6.
• `day_of_month` is the wildcard (*) for every day in the month.
• `month` is the wildcard (*) for every month.
• `day_of_week` is the wildcard (*) for every day in the week.

• To set 06:34 in a time range, enter the `absolute 06:34 * * 2009` and the `periodic 06:34` interface configuration commands.

Note
When configuring recurrences, do not schedule multiple recurrence events to start at the same time. We recommend that you configure events at least 15 minutes apart.

Day of the Month and Day of the Week Recurrences
When you use the `day_of_month` and the `day_of_week` variables in the `energywise level level recurrence importance importance at minute hour day_of_month month day_of_week` interface configuration command, follow these guidelines:

• The recurrence occurs when either the `day_of_month` or the `day_of_week` occurs first (in releases earlier than the Cisco EnergyWise Version 2.7 releases). See the Release Notes for Cisco EnergyWise, EnergyWise Version 2.7 on Cisco.com for software releases with Cisco EnergyWise Version 2.7.

• If you specify both the `day_of_month` and the `day_of_week`, the event occurs when either the `day_of_month` or the `day_of_week` is first.

• If you specify the `day_of_month` and use a wildcard (*) for the `day_of_week`, the event occurs on the `day_of_month`.

• If you use a wildcard for the `day_of_month` and specify the `day_of_week`, the event occurs on the `day_of_week`.

• If you use wildcards for both the `day_of_month` and the `day_of_week`, the event occurs on any day.
Queries

The management station sending a query receives all the power-usage responses from the EnergyWise domain. The domain members use neighbor relationships to forward the query.

For secure communication, the domain members use a shared secret and send only authenticated queries to the endpoints.

*Figure 37: Query Requests and Replies*

![Diagram showing query requests and replies](image)

*Table 48: Query Requests and Replies*

<table>
<thead>
<tr>
<th>Number</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The management station sends queries and messages to the domain.</td>
</tr>
<tr>
<td>2</td>
<td>The domain member replies to queries and messages from the management station.</td>
</tr>
<tr>
<td>3</td>
<td>The domain member sends queries and messages to other domain members and endpoints.</td>
</tr>
<tr>
<td>4</td>
<td>The domain member replies to queries and messages from other domain members and endpoints.</td>
</tr>
</tbody>
</table>

EnergyWise supports the following query types:

- **Collect**—Receives power-usage information in watts (W) from the domain members and endpoints.
- **Save**—Saves the running configuration of a domain member. Use the `energywise allow query save` global configuration command.
- **Set**—Changes the power level of a domain member or endpoint in the running configuration.
- **Sum**—Summarizes the information from domain members and endpoints.

You can use these attributes to filter the results:
• Importance—Rate your devices based on the business or deployment context. For example, a desk phone has a lower importance than a business-critical emergency phone. The range is from 1 (least important) to 100 (most important). The default is 1.

• Keywords—Describes the device (other than the name or role).

• Name—Identifies the device.

• Role—Specifies the device function based on the business or deployment context.

• Usage—Specifies the energy usage type of the Cisco EnergyWise device. The default is consumer.
  • All—Devices of all usage types.
  • Consumer—A device that consumes power, such as a switch.
  • Meter—A device that measures the pass-through power, such as a power distribution unit (PDU) that sends power from a source to a connected device.
  • Producer—A device that generates power, such as a solar panel.

The query results show domain members and endpoints with importance values less than or equal to the specified value in the query.

Related Topics
  Examples: Querying to Analyze Domains, on page 409
  Examples: Querying with the Name Attribute, on page 409
  Examples: Querying with Keywords, on page 410
  Examples: Querying to Set Power Levels, on page 410

Activity Check

You can use this feature to ensure that the switch does not power off a phone that is in use. For example, if you have a Cisco IP phone connected to a PoE port and activity check is enabled, the switch does not power off the phone if it is sending or receiving voice traffic. If the phone is not in use, it powers off within approximately 1 minute. If a PC is connected to the switch port of the phone, the PC loses network connectivity when the phone is powered off.

You can configure activity check on these Cisco devices:
  • Cisco Catalyst 4500 and 6500 series switches.
  • Cisco Industrial Ethernet (IE) 2000, 3000, and 3010 series switches.

Related Topics
  Configuring Activity Check, on page 400
Wake on LAN

Wake on LAN (WoL) is an Ethernet computer networking standard that uses a network message called a magic packet to wake up an endpoint device. The magic packet contains the MAC address of the destination endpoint device (typically a PC). For example, you can send a WoL magic packet to a PC. The listening PC waits for a magic packet addressed to it and then initiates the system to wake up.

WoL is implemented on the motherboard (BIOS) and the network interface. It is operating-system independent. WoL could be disabled by default on some PCs.

**Related Topics**
- Using WoL with a MAC Address, on page 401
- Using WoL Without a MAC Address, on page 402
- Prerequisites for Wake on LAN, on page 375

WoL with Cisco EnergyWise

You can configure the EnergyWise domain member to send a WoL magic packet to a specific endpoint device or all endpoint devices in the EnergyWise network. When a WoL-enabled PC is connected to the domain member, it receives the WoL magic packet and the power level of the PC changes from nonoperational to operational.

Some network interface cards (NICs) have a SecureOn feature with which you can store a hexadecimal password within the NIC. When you send WoL packets to NICs with SecureOn, the NICs store this password as part of the packet, making the wake up process secure. If the PC you are trying to wake up has an NIC that supports SecureOn, the domain member must send a magic packet with the hexadecimal password to power on the PC.

Configuration Guidelines

Enabling Cisco EnergyWise and Powering Devices

By default, Cisco EnergyWise is disabled on the domain member.

If you enter the `no energywise level` interface configuration command, the domain member does not immediately change to the default power level. The power level changes when you restart the domain member or enter the `energywise level level` command.

**Domain Member with PoE Ports**

For a domain member with PoE ports, such as a PoE-capable switch:

- When you add an endpoint to an EnergyWise domain, it becomes an EnergyWise domain member and EnergyWise is enabled on the new domain member and all the PoE ports.

- When you use the `energywise level 0` interface configuration command, the port does not provide power to connected endpoints.

- You cannot use the `energywise level 0` global configuration command to power off the domain member.
Error-Disabled Ports

If a port is error-disabled:

- It appears as an EnergyWise domain member or endpoint in the `show` command output and in the `collect` query results. The query results show that the port uses 0 watts.

- It does not respond to a `set` query.

PoE and EnergyWise Interactions

You can configure EnergyWise on the port and configure the port power level.

The following table shows you how to find out if a domain member port participates in Cisco EnergyWise. For each combination of port and PoE mode check the matrix entry, if it is `Yes`, then the port participates in Cisco EnergyWise; if it is `No`, then the port does not participate in EnergyWise.

For example, if the port is PoE and the PoE mode is `never`, the table matrix entry is `No`; this means Cisco EnergyWise is not disabled even if the port power is off.

Table 49: Domain Member Port Participation in Cisco EnergyWise

<table>
<thead>
<tr>
<th>Port</th>
<th>PoE Mode—auto</th>
<th>PoE Mode—never</th>
<th>PoE mode—static</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-PoE</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

When you change the port mode using the `power inline auto` or `power inline static` interface configuration commands, changes are effective immediately. You do not need to restart the domain member.

If Cisco EnergyWise is disabled, the domain member can use PoE to manage the port power usage.

When you configure a recurrence for PoE interfaces, EnergyWise functions the same way as when the `power inline` and `no power inline` interface configuration commands are executed. You might see messages that show the interface going up and down at time of the event.

CLI Compatibility

Follow these guidelines for EnergyWise to work properly:

- All domain members must run Cisco EnergyWise Version 1 or Cisco EnergyWise Version 2.6 or later.

- All domain members must have the same domain name and security mode.

- If your switch is stacking-capable and is a member of a switch stack, all the stack members must run the same Cisco EnergyWise version.

- If your domain member is running Cisco EnergyWise Version 1, and you upgrade your software to a release supporting Cisco EnergyWise Version 2.6 or later:
  - The EnergyWise settings in the running configuration are updated. The domain member sets the management password as the same domain password in the `energywise domain` command.
  - Enter the `copy running-config startup-config` privileged EXEC command to save the EnergyWise settings in the configuration file.
• If your domain member is running Cisco EnergyWise Version 2.6 or later and you need to downgrade to Cisco EnergyWise Version 1.0 due to domain member compatibility issues, enter the `no energywise domain` global configuration command to disable EnergyWise before downgrading your software to a release supporting EnergyWise Version 1.

To display the Cisco EnergyWise version running on your domain member, use the `show energywise version` privileged EXEC command. The Cisco EnergyWise version is referred to as the EnergyWise specification in the command output.

To display the software version running on your domain member, use the `show version` privileged EXEC command.

In Cisco EnergyWise Version 1, these commands were modified:

• `energywise domain domain-name secret [0 | 7] password` global configuration command

  We recommend that you reconfigure the EnergyWise domain with the `energywise domain domain-name security {ntp-shared-secret | shared-secret} [0 | 7] shared-secret [protocol udp port udp-port-number [interface interface-id | ip ip-address]]` global configuration command.

  If you do not reconfigure the domain, the domain member synchronizes the management password with the domain password.

• `energywise management tcp-port-number` global configuration command

  We recommend that you reconfigure the management password for the domain with the `energywise management security shared-secret [0 | 7] shared-secret port tcp-port-number` global configuration command.

---

How to Configure EnergyWise

Enabling Cisco EnergyWise

**SUMMARY STEPS**

1. configure terminal
2. service password-encryption
3. `energywise domain domain-name security {ntp-shared-secret | shared-secret} [0 | 7] domain-password [protocol udp port udp-port-number [interface interface-id | ip ip-address]]`
4. end
5. show energywise
6. show energywise domain
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainMember# configure terminal</td>
</tr>
</tbody>
</table>

### Purpose

- **DomainMember# configure terminal**

### Step 2

**service password-encryption**

**Example:**

```plaintext
DomainMember(config)# service password-encryption
```

(Optional) Enables password encryption.

If you set a hidden password in Step 3, enter this command.

### Step 3

**energywise domain domain-name security**

- ntp-shared-secret [shared-secret] [0 | 7]
- domain-password [protocol udp port udp-port-number]
- interface interface-id | ip ip-address]

**Example:**

```plaintext
DomainMember(config)# energywise domain cisco security shared-secret cisco protocol udp port 43440 ip 2.2.4.30
```

Enables Cisco EnergyWise on the network device, assigns it to a domain with the specified domain-name, sets the domain security mode, and sets the domain password to authenticate all communication in the domain.

- **ntp-shared-secret**—Sets a strong password with NTP. If the time between members varies ±30 seconds, the domain member drops events.
- **shared-secret**—Sets a strong password without NTP.

* (Optional) **0**—Uses a plain-text password. This is the default.

* (Optional) **7**—Uses a hidden password.

If you do not enter 0 or 7, the default is 0.

* (Optional) **port udp-port-number**—Specifies the UDP port that communicates with the domain.

The range is from 1 to 65000. The default is 43440.

* (Optional) **interface interface-id**—Specifies the port that communicates with the domain if the IP address is dynamically assigned. We recommend that you specify the interface-id value. You should use this in a bridged network.

* (Optional) **ip ip-address**—Specifies the IP address that communicates with the domain if the interface is a switched virtual interface (SVI) and VLAN trunking protocol (VTP) pruning is enabled. You should use this in a routed network.

For the **domain-name** and **domain-password**:

- You can enter alphanumeric characters and symbols such as #, $, !, and &.
- Do not enter an asterisk (*) or a space between the characters or symbols.

### Step 4

**end**

**Example:**

```plaintext
DomainMember(config)# end
```

Returns to privileged EXEC mode.
### Configuring Domain Member or Endpoint Attributes

#### SUMMARY STEPS

1. `configure terminal`
2. `energywise importance importance`
3. `energywise keywords word, word, word...`
4. `service password-encryption`
5. `energywise management security shared-secret [ 0 | 7 ] mgmt-password [port tcp-port-number]`
6. `energywise name name`
7. `energywise neighbor [hostname | ip-address] udp-port-number`
8. `energywise role role`
9. `energywise allow query [save | set]`
10. `energywise endpoint security [none | shared-secret [0 | 7] shared-secret]`
11. `end`
12. `show energywise`
13. `show energywise domain`
14. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>DomainMember# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>energywise importance importance</code></td>
<td>Sets the importance.</td>
</tr>
<tr>
<td>Example: <code>DomainMember(config)# energywise importance 65</code></td>
<td>The range is from 1 to 100. The default is 1.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>energywise keywords word, word, word...</code></td>
<td>Assigns at least one keyword.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Example:**  
DomainMember(config)# energywise keywords  
lab1, devlab | When assigning multiple keywords, separate the keywords with commas, and do not use spaces between keywords.  
- You can enter alphanumeric characters and symbols such as #, $, !, and &.  
- Do not enter an asterisk (*) or a space between the characters or symbols.  
By default, keywords are not defined. |

| **Step 4** | **service password-encryption** | (Optional) Enables password encryption.  
If you set a hidden password in Step 3, enter this command. |
| **Example:**  
DomainMember(config)# service password-encryption | |

| **Step 5** | **energywise management security shared-secret [ 0 | 7]**  
**mgmt-password [port tcp-port-number]** | Sets the management password on the domain member that the management station uses to communicate with the domain.  
- (Optional) 0—Uses a plain-text password.  
- (Optional) 7—Uses a hidden password.  
If you do not enter 0 or 7, the default is 0.  
For the mgmt-password:  
- You can enter alphanumeric characters and symbols such as #, $, !, and &.  
- Do not enter an asterisk (*) or a space between the characters or symbols.  
(Optional) port tcp-port-number—Specifies the TCP port for management access. The range is from 1025 to 65535. The default is 43440.  
By default, the management password is not set. |
| **Example:**  
DomainMember(config)# energywise management  
security shared-secret cisco port 1055 | |

| **Step 6** | **energywise name name** | Specifies the EnergyWise-specific name.  
- You can enter alphanumeric characters and symbols such as #, $, !, and &.  
- Do not enter an asterisk (*) or a space between the characters or symbols.  
The default is the host name. |
| **Example:**  
DomainMember(config)# energywise name LabSwitch | |

| **Step 7** | **energywise neighbor [ hostname | ip-address ]**  
**udp-port-number** | Assigns a static neighbor.  
- Domain Name System (DNS) hostname (hostname) or IP address (ip-address). |
| **Example:**  
DomainMember(config)# energywise neighbor member1  
43440 | |
## Configuring EnergyWise

### Configuring Domain Member or Endpoint Attributes

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> energywise role <em>role</em></td>
<td>Specifies the role in the EnergyWise domain. For example, lobby.b20.</td>
</tr>
<tr>
<td><strong>Example:</strong> DomainMember(config)# energywise role role.labaccess</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> energywise allow query [save</td>
<td>set]</td>
</tr>
<tr>
<td><strong>Example:</strong> DomainMember(config)# energywise allow query save</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> energywise endpoint security [ none</td>
<td>shared-secret [ 0</td>
</tr>
<tr>
<td><strong>Example:</strong> DomainMember(config)# energywise endpoint security shared-secret cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> DomainMember(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Purpose

- **Command or Action:**
- **Purpose:**
  - **Purpose:**
    - UDP port (*udp-port-number*) that sends and receives queries.
      - The range is from 1 to 65000.
    - By default, static neighbors are not assigned.
  - **Purpose:**
    - Specifies the role in the EnergyWise domain. For example, lobby.b20.
    - You can enter alphanumeric characters and symbols such as #, $, !, and &.
    - Do not enter an asterisk (*) or a space between the characters or symbols.
    - The default is the model number.
  - **Purpose:**
    - Configures the domain member to respond to queries from the management station or another domain member.
    - *save*—Responds to a query to save the running configuration.
    - *set*—Responds to a query to change the power level or the EnergyWise attributes.
    - By default, the domain member responds to the set query.
  - **Purpose:**
    - Sets the security mode for an endpoint.
    - *none*—Disables security.
    - *shared-secret*—Uses a password for secure communication with the domain member.
      - (Optional) 0—Uses a plain-text password.
      - (Optional) 7—Uses a hidden password.
      - If you do not enter 0 or 7, the default is 0.
      - For the shared-secret:
        - You can enter alphanumeric characters and symbols such as #, $, !, and &.
        - Do not enter an asterisk (*) or a space between the characters or symbols.
      - By default, the password is not set.
  - **Purpose:**
    - Returns to privileged EXEC mode.
### Powering the PoE Port

**SUMMARY STEPS**

1. `configure terminal`  
2. `interface interface-id`  
3. `energywise level level`  
4. `end`  
5. `show energywise`  
6. `show energywise domain`  
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
| Example:  

```
DomainMember# configure terminal
``` | |
| **Step 2** | Specifies the port or the range of ports to be configured and enters interface configuration mode. |
| `interface interface-id` | |
| Example:  

```
DomainMember(config)# interface gigabitethernet1/0/2
``` | |
| **Step 3** | Manually powers on the port. |
| `energywise level level` | |
| Example:  

```
``` | |
### Configuring Port Attributes

**Before you begin**

Before entering the `energywise activitycheck` command in Step 7:

- Verify that automatic quality of service (auto-QoS) is enabled on the port and on the connected IP phone.
- If the domain member is connected to the IP phones through multiple Cisco devices, verify that they trust the CoS value in the incoming packets.

For more information about activity check and configuring auto-QoS, see *Activity Check, on page 383.*

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. energywise importance importance
4. energywise keywords word, word, word...
5. energywise name name
6. energywise role role

---

### Configuring EnergyWise

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| DomainMember(config-if)# **energywise level 3** | • For a connected PoE endpoint, enter a power level of 10.  
• For an non-PoE-capable endpoint, enter a power level from 1 to 10. The endpoint determines the appropriate action. |

**Step 4**

*Example:*

DomainMember(config-if)#**end**

Returns to privileged EXEC mode.

**Step 5**

*Example:*

DomainMember# **show energywise**

Verifies your entries.

**Step 6**

*Example:*

DomainMember# **show energywise domain**

Verifies your entries.

**Step 7**

*Example:*

DomainMember# **copy running-config startup-config**

(Optional) Saves your entries in the configuration file.

**Note**

The power level that you set in Step 3 is the default power level when the domain member restarts.
### Configuring EnergyWise

#### Configuring Port Attributes

1. configure terminal

   **Example:**
   ```
   DomainMember# configure terminal
   ```

2. interface interface-id

   **Example:**
   ```
   DomainMember(config)# interface gigabitethernet1/0/2
   ```

3. energywise importance importance

   **Example:**
   ```
   DomainMember (config-if)# energywise importance 90
   ```

4. energywise keywords word, word, word...

   **Example:**
   ```
   DomainMember (config-if)# energywise keywords lab
   ```

5. energywise name name

   **Example:**
   ```
   DomainMember (config-if)# energywise name labphone.5
   ```

6. energywise role role

   **Example:**
   ```
   DomainMember (config-if)# energywise role role.labphone
   ```

---

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **configure terminal**  
  **Example:**
  ```
  DomainMember# configure terminal
  ``` | Enters the global configuration mode. |
| **Step 2** | **interface interface-id**  
  **Example:**
  ```
  DomainMember(config)# interface gigabitethernet1/0/2
  ``` | Specifies the port or the range of ports to be configured, and enters interface configuration mode. |
| **Step 3** | **energywise importance importance**  
  **Example:**
  ```
  DomainMember (config-if)# energywise importance 90
  ``` | Sets the importance.  
  The range is from 1 to 100. The default is 1. |
| **Step 4** | **energywise keywords word, word, word...**  
  **Example:**
  ```
  DomainMember (config-if)# energywise keywords lab
  ``` | Assigns at least one keyword.  
  When assigning multiple keywords, separate the keywords with commas, and do not use spaces between keywords.  
  - You can enter alphanumeric characters and symbols such as #, $, !, and &.  
  - Do not enter an asterisk (*) or a space between the characters or symbols.  
  By default, keywords are not defined. |
| **Step 5** | **energywise name name**  
  **Example:**
  ```
  DomainMember (config-if)# energywise name labphone.5
  ``` | Specifies the EnergyWise-specific name.  
  - You can enter alphanumeric characters and symbols such as #, $, !, and &.  
  - Do not enter an asterisk (*) or a space between the characters or symbols.  
  The default is the host name. |
| **Step 6** | **energywise role role**  
  **Example:**
  ```
  DomainMember (config-if)# energywise role role.labphone
  ``` | Specifies the role in the EnergyWise domain. For example, lobby.b20.  
  - You can enter alphanumeric characters and symbols such as #, $, !, and &. |
### Command or Action | Purpose
--- | ---
|  |  • Do not enter an asterisk (*) or a space between the characters or symbols. The default is the model number.

**Step 7** energywise activitycheck  
**Example:**  
```
DomainMember (config-if)# energywise activitycheck
```  
Verifies that the connected IP phone is not sending or receiving traffic before the domain member powers off the port.  
**Note** The domain member cannot determine if the IP phone is in the hold state.

**Step 8** energywise allow query set  
**Example:**  
```
DomainMember (config-if)# energywise role role.labphone
```  
If the interface receives a query from the management station or another domain member, configures the interface to respond to a query changing the power level and the EnergyWise attributes.  
By default, the domain member responds to this query.

**Step 9** end  
**Example:**  
```
DomainMember (config-if)# end
```  
Returns to privileged EXEC mode.

**Step 10** show running-config  
**Example:**  
```
DomainMember# show running-config
```  
Verifies your entries.

**Step 11** copy running-config startup-config  
**Example:**  
```
DomainMember# copy running-config startup-config
```  
(Optional) Saves your entries in the configuration file.

**Related Topics**

- [Attributes](#), on page 379

## Configuring Recurrences

**SUMMARY STEPS**

1. show energywise  
2. configure terminal  
3. time-range time-range-name  
4. absolute start hh:mm day_of_month month year  
5. periodic days_of_the_week hh:mm  
6. interface interface-id  
7. energywise level level recurrence importance importance {at minute hour day_of_month month day_of_week | time-range time-range-name}  
8. end
9. show energywise recurrence
10. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show energywise</td>
<td>Verifies that EnergyWise is enabled.</td>
</tr>
<tr>
<td>Example:</td>
<td>DomainMember# show energywise</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>DomainMember# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>time-range time-range-name</td>
<td>Assigns a name to the time range, and enters the time-range configuration mode. If you do not configure a time range, go to Step 6.</td>
</tr>
<tr>
<td>Example:</td>
<td>DomainMember(config)# time-range onfirstfloor</td>
<td></td>
</tr>
</tbody>
</table>

**Therange is based on the system clock.**

- If EnergyWise is not running on the endpoint (for example, a PoE endpoint), the specified times are based on the domain member time zone.
- If an agent or client is running on the endpoint, the specified times are based on the endpoint time zone.

Use the **absolute** and the **periodic** time-range configuration commands to specify times and days for a recurrence. You can use one absolute condition and multiple periodic conditions.

| Step 4 | absolute start hh:mm day_of_month month year | Sets the start time and day for the recurrence. If the **absolute** condition has an end time and day, the domain member ignores these values. |
| Example: | DomainMember(config-time-range)# absolute start 0:00 1 August 2009 |

- **hh:mm**—Specifies the time (24-hour format) in hours and minutes.
- **day month year**—Specifies the date.
  - **day_of_month**—The range is from 1 to 31.
  - **month**—The range is from January to December.
  - **year**—The minimum year is 1993.

When configuring the absolute time range, the wild card * option is not supported for **day_of_month** and **month**.

| Step 5 | periodic days_of_the_week hh:mm | Sets the weekly start time and day for the recurrence. |
| Example: | |

- **days_of_the_week**—Valid values:
## Configuring Recurrences

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainMember(config-time-range)# <strong>periodic weekdays</strong> 06:00 to 22:00</td>
<td>• <strong>Monday</strong>, <strong>Tuesday</strong>, <strong>Wednesday</strong>, <strong>Thursday</strong>, <strong>Friday</strong>, <strong>Saturday</strong>, or <strong>Sunday</strong>—Enter a single day, a range of days with a dash between the starting and ending days, or multiple days separated by a comma.</td>
</tr>
<tr>
<td>DomainMember(config-time-range)# <strong>periodic weekend</strong> 10:00 to 16:00</td>
<td>• <strong>daily</strong>—Enter if the recurrence starts from Monday to Sunday.</td>
</tr>
<tr>
<td>Step 6</td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies the port or a range of ports to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>DomainMember(config)# <strong>interface</strong> gigabitethernet1/0/2</td>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• <strong>level level</strong>—Specifies the power level.</td>
</tr>
<tr>
<td>DomainMember(config-if)# <strong>energywise level</strong> 10 <strong>recurrence importance</strong> 70 <strong>time-range</strong> onfirstfloor</td>
<td>• To power off the endpoint, enter 0.</td>
</tr>
<tr>
<td></td>
<td>• To power on the endpoint:</td>
</tr>
<tr>
<td></td>
<td>If it is a PoE endpoint, enter 10.</td>
</tr>
<tr>
<td></td>
<td>If it is another powered device, enter a power level from 1 to 10. The endpoint determines the appropriate action.</td>
</tr>
<tr>
<td></td>
<td>• <strong>importance importance</strong>—The event occurs if the importance value of the endpoint is less than or equal to the importance value. The range is from 1 to 100.</td>
</tr>
<tr>
<td></td>
<td>• <strong>at minute hour day_of_month month day_of_week</strong>—Specifies the time (24-hour format) in cron format for the recurrence.</td>
</tr>
<tr>
<td></td>
<td>• <strong>minute</strong>—The range is from 0 to 59. Use * for the wildcard.</td>
</tr>
<tr>
<td></td>
<td>• <strong>hour</strong>—The range is from 0 to 23. Use * for the wildcard.</td>
</tr>
<tr>
<td></td>
<td>• <strong>day_of_month</strong>—The range is from 1 to 31. Use * for the wildcard.</td>
</tr>
</tbody>
</table>
Purpose

- **month**—The range is from 1 (January) to 12 (December). Use * for the wildcard.
- **day_of_week**—The range is from 0 (Sunday) to 6 (Saturday). Use * for the wildcard.
- **time-range** **time-range-name**—Specifies the time range for the recurrence.

The event uses the domain member time.
Repeat this step to schedule another event.

**SUMMARY STEPS**

1. energywise query analyze domain **domain-name**
2. energywise query importance **importance** {**keywords** **word**, **word**, ... | **name** **name**} **collect** {**delta** | **usage**} {all | consumer | meter | producer} {**timeout** **timeout**}
3. **energywise query importance** importance \{keywords word, word,... | name name\} \sum \{delta | usage\} \left[ all \left[ \text{timeout timeout} \right] \right] \left[ consumer \left[ \text{timeout timeout} \right] \right] \left[ meter \left[ \text{timeout timeout} \right] \right] \left[ producer \left[ \text{timeout timeout} \right] \right] \left[ timeout timeout \right] \]

4. **energywise query importance** importance \{keywords word, word,... | name name\} \texttt{set level level} \left[ all \left[ \text{timeout timeout} \right] \right] \left[ consumer \left[ \text{timeout timeout} \right] \right] \left[ meter \left[ \text{timeout timeout} \right] \right] \left[ producer \left[ \text{timeout timeout} \right] \right] \left[ timeout timeout \right] \]

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> energywise query analyze domain \textit{domain-name}</td>
<td>Runs a query to analyze and display information about the domain, including the domain size and the number of members and endpoints.</td>
</tr>
<tr>
<td>Example: DomainMember# energywise query analyze domain</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> energywise query importance importance {keywords word, word,...</td>
<td>name name} \texttt{collect} {delta</td>
</tr>
<tr>
<td>Example: DomainMember# energywise query importance 100 name * collect usage consumer</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• (Optional) <strong>all</strong>—Displays EnergyWise devices of all usage types.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>consumer</strong>—Filters the results to display devices that consume power, such as a switch. This is the default usage type.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>meter</strong>—Filters the results to display devices that measure the pass-through power, such as a PDU that sends power from a source to a connected device.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>producer</strong>—Filters the results to display devices that generate power, such as a solar panel.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>timeout timeout</strong>—Sets the time in seconds that the management station waits for query results. When configuring the timeout, configure a minimum of 6 seconds to display correct output.</td>
<td></td>
</tr>
</tbody>
</table>

The default **timeout** is 6 seconds. The range is from 1 to 180.

Repeat this step to run another query.

### Step 3

**energywise query importance importance {keywords word, word,... | name name} sum {delta | usage} [all [timeout timeout] | consumer [timeout timeout] | meter [timeout timeout] | producer [timeout timeout] | timeout timeout]**

**Example:**

```
DomainMember# energywise query importance 90 keyword lobby sum usage
```

You can perform Step 2 or Step 3

### Step 4

**energywise query importance importance {keywords word, word,... | name name} set level level [all [timeout timeout] | consumer [timeout timeout] | meter [timeout timeout] | producer [timeout timeout] | timeout timeout]}**

**Example:**

```
DomainMember# energywise query importance 80 name shipping.2 set level 0
```

(Optional) Runs a query to change the power level and to power on or off the domain members, PoE ports, or endpoints.

**Note** Use this query with care. It affects both the domain member on which you enter the command and other domain members and endpoints that match the query criteria.

• **importance importance**—Filters the results based on the importance value. Only domain members and endpoints with values less than or equal to the specified value appear. The range is from 1 to 100.

• **keywords word, word...**—Filters the results based on one or more keywords.

**Note** Do not run a query with **keywords***. No results are generated.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>name name</strong>—Filters the results based on the name. For the wildcard, use * or name* with the asterisk at the end of the name phrase.</td>
<td></td>
</tr>
<tr>
<td>• <strong>set level level</strong>—Sets the power level of the domain members, endpoints, or PoE ports. The range is from 0 to 10.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>all</strong>—Displays EnergyWise devices of all usage types.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>consumer</strong>—Filters the results to display devices that consume power, such as a switch. This is the default usage type.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>meter</strong>—Filters the results to display devices that measure the pass-through power, such as a PDU that sends power from a source to a connected device.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>producer</strong>—Filters the results to display devices that generate power, such as a solar panel.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) <strong>timeout timeout</strong>—Sets the time in seconds that the management station waits for query results. When configuring the timeout, configure a minimum of 6 seconds to display correct output.</td>
<td></td>
</tr>
</tbody>
</table>

The default is 6 seconds. The range is from 1 to 180. Repeat this step to run another query.

---

### Configuring Activity Check

#### SUMMARY STEPS

1. **configure terminal**
2. **interface interface-id**
3. **energywise activity check**

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **configure terminal**
| Example: | DomainMember# configure terminal |

Enters the global configuration mode.

| **Step 2** | **interface interface-id**
| Example: | |

Specifies the port or a range of ports to be configured, and enters the interface configuration mode.
In the examples, the interface-id is in this format: type slot-or-module-number/port-number, for example, gigabitethernet 0/5. To specify an interface, see your device software documentation.

Step 3
energywise activity check

Example:
DomainMember(config-if)# energywise activitycheck

Configure the domain member to wait until a Cisco IP phone connected to a PoE port is not sending or receiving traffic before the domain member powers off the port.

Note: The domain member cannot determine if the IP phone is in the hold state.

What to do next
Proceed to test activity check.

Related Topics
Activity Check, on page 383

Testing Activity Check

After you have enabled activity check, perform the following checks to make sure that the switch powers off the port only when a connected Cisco IP phone is not sending or receiving voice traffic.

While making a phone call, set the port power level to 0. The switch should not power off the IP phone. To set the port power level, you can:

- Run a query (using the CLI or the management application programming interface [MAPI]) — The switch performs an activity check before powering off.
- Use a recurrence — The switch performs an activity check before powering off.
- Use the CLI — The switch does not perform an activity check and powers off the PoE port immediately.

Using WoL with a MAC Address

SUMMARY STEPS

1. energywise query importance importance {keywords word, word,... | name name} wol mac mac-address [password password | port tcp-port-number [password password]]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> energywise query importance importance {keywords word, word,...</td>
<td>name name} wol mac mac-address [password password</td>
</tr>
<tr>
<td></td>
<td>• importance importance — Only domain members and endpoints with importance values less than or equal</td>
</tr>
</tbody>
</table>
### Related Topics

- [Wake on LAN](#), on page 384
- [Prerequisites for Wake on LAN](#), on page 375

## Using WoL Without a MAC Address

To use WoL without entering a MAC address, first configure the EnergyWise endpoint device to include off-state caching and WoL. To wake up the device and set its power level, use the `energywise query privileged EXEC` command. For example, enter this command:

```
DomainMember# energywise query importance 100 keywords pc set level 10
```

Device MAC addresses are cached along with their keywords or names. The domain member matches the keywords or name you enter with the cached keywords, names, and MAC addresses and sends the WoL packet to the matching device.

The WoL packet is sent only if the device is powered off.
Related Topics
- Wake on LAN, on page 384
- Prerequisites for Wake on LAN, on page 375

Monitoring and Troubleshooting EnergyWise

Monitoring EnergyWise

Use the following commands to monitor EnergyWise.

Table 50: show Privileged EXEC Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show energywise</td>
<td>Displays the settings and status for the domain member or endpoint.</td>
</tr>
<tr>
<td>show energywise children</td>
<td>Displays the status of the connected endpoints.</td>
</tr>
<tr>
<td>show energywise provisioned</td>
<td>Displays a summary of the EnergyWise information for the domain member and the connected endpoints.</td>
</tr>
<tr>
<td>show energywise domain</td>
<td>Displays the domain to which the domain member or endpoint belongs.</td>
</tr>
<tr>
<td>show energywise events</td>
<td>Display the last ten events (messages) sent to other domain members or endpoints in the domain.</td>
</tr>
<tr>
<td>show energywise neighbor</td>
<td>Displays the neighbor tables for the domain member.</td>
</tr>
<tr>
<td>show energywise recurrences</td>
<td>Displays the EnergyWise settings and status for recurrence.</td>
</tr>
<tr>
<td>show energywise statistics</td>
<td>Displays the counters for events and errors.</td>
</tr>
<tr>
<td>show energywise usage</td>
<td>Displays the actual power usage on the domain member or endpoint.</td>
</tr>
<tr>
<td>show energywise version</td>
<td>Displays the EnergyWise version.</td>
</tr>
<tr>
<td>show version</td>
<td>Displays the software version.</td>
</tr>
<tr>
<td>show power inline</td>
<td>Displays the PoE status.</td>
</tr>
<tr>
<td>show cdp neighbors</td>
<td>Displays the neighbors discovered by CDP.</td>
</tr>
</tbody>
</table>

Verifying Power Usage

This example shows you how to verify that the Cisco 7960 IP Phone uses 6.3 W and that the Cisco 7970G IP Phone uses 10.3 W:

```
Switch# show energywise usage children
Interface Name Usage Caliber
--------- ---- ----- -------
Switch 144.0 (W) max
```
Detecting Communication Failures

Use the EnergyWise debug mode commands to show communication failures.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug energywise debug</td>
<td>Displays errors such as invalid sequence numbers and communication errors on the domain.</td>
</tr>
<tr>
<td>debug energywise discovery</td>
<td>Displays all EnergyWise discovery information.</td>
</tr>
<tr>
<td>debug energywise endpoint</td>
<td>Displays information about EnergyWise endpoints running a client or agent and helps detect mismatched domain names, secrets, and sequence numbers of connected endpoints.</td>
</tr>
<tr>
<td>debug energywise ha</td>
<td>Displays EnergyWise high availability (HA) information for devices that have HA capability.</td>
</tr>
<tr>
<td>debug energywise management</td>
<td>Displays information about authentication failures and EnergyWise management stations running power management applications.</td>
</tr>
<tr>
<td>debug energywise packet</td>
<td>Displays EnergyWise packet trace information.</td>
</tr>
<tr>
<td>debug energywise query</td>
<td>Displays query information relating to the device from which the query is initiated.</td>
</tr>
<tr>
<td>debug energywise trace</td>
<td>Displays information about all the EnergyWise processes relating to the device from which the query is initiated.</td>
</tr>
<tr>
<td>debug energywise wol</td>
<td>Displays Wake on LAN (WoL) query information relating to the device from which the query is initiated.</td>
</tr>
</tbody>
</table>

Disabling EnergyWise

To disable EnergyWise, enter the interface configuration commands followed by the global configuration commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no energywise</td>
<td>Disables EnergyWise on the PoE port or on the endpoint.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>no energywise activitycheck</td>
<td>Configures the domain member not to wait until a Cisco IP phone connected to a PoE port is not sending or receiving voice traffic before the domain member powers off the port.</td>
</tr>
<tr>
<td>no energywise allow query set</td>
<td>Configures the interface to drop all set queries for the interface and children. If configured, you cannot change the power level or EnergyWise attributes of connected devices on the interface. To prevent power levels on all interfaces from being changed, apply the command to all interfaces.</td>
</tr>
<tr>
<td>no energywise [ importance</td>
<td>keywords [ word, word, ...] ] level</td>
</tr>
<tr>
<td>no energywise level level recurrence importance [ at minute hour day_of_month month day_of_week</td>
<td>timerange timerange-name}</td>
</tr>
<tr>
<td>Table 53: Global Configuration Commands for Disabling EnergyWise</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>no energywise allow query save</td>
<td>Configures the domain member not to respond to a query that saves the running configuration.</td>
</tr>
<tr>
<td>no energywise allow query set</td>
<td>Configures the domain member to drop all set queries for the parent entity. If configured, you cannot change the power level or EnergyWise attributes of the domain member. This configuration does not apply to the interfaces or endpoints connected to any interfaces.</td>
</tr>
<tr>
<td>no energywise domain</td>
<td>Disables EnergyWise on the domain member.</td>
</tr>
<tr>
<td>no energywise endpoint</td>
<td>Configures the domain member not to establish parent-child relationships with connected EnergyWise-compatible endpoints. The endpoints cannot receive queries or messages from the domain member.</td>
</tr>
<tr>
<td>no energywise [ importance</td>
<td>keywords [ word, word, ...] ] name</td>
</tr>
</tbody>
</table>
Configuration Examples for EnergyWise

Examples: Setting the Domain

The following example displays how to set the domain:

```
DomainMember# show energywise
Interface Role Name Usage Lvl Imp Type
--------- ---- ---- ----- --- --- ----
fanfare jsmith 1009.0(W) 5 100 paren

DomainMember# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DomainMember(config)# energywise domain cisco security ntp-shared-secret cisco protocol udp port 43440 ip 2.2.4.30
DomainMember(config)# energywise importance 50
DomainMember(config)# energywise keywords lab1,devlab
DomainMember(config)# energywise name LabSwitch
DomainMember(config)# energywise neighbor member1 43440
DomainMember(config)# energywise role role.labaccess
DomainMember(config)# energywise allow query save
DomainMember(config)# end
```

```
DomainMember# show energywise domain
Name : member1
Domain : cisco
Protocol : udp
IP : 2.2.2.21
Port : 43440

DomainMember# show energywise neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Id Neighbor Name Ip:Port Prot Capability
-- ------------- ------- ---- ----------
1 member-21 2.2.2.21:43440 udp S I
2 member-31 2.2.4.31:43440 static S I
3 member-22 2.2.2.22:43440 cdp S I
```

Related Topics
- Configuring Domain Member or Endpoint Attributes, on page 388
- EnergyWise Domain, on page 377

Examples: Manually Managing Power

The following example displays how to manually manage the power.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no energywise management</td>
<td>Configures the domain member to not communicate with a connected management station that sends queries.</td>
</tr>
</tbody>
</table>
To power on the lab IP phones:

DomainMember# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DomainMember(config)# energywise domain cisco security shared-secret cisco protocol udp port 43440 ip 2.2.4.44
domainMember(config)# interface gigabitethernet0/3
DomainMember(config-if)# energywise importance 65
DomainMember(config-if)# energywise name labphone.5
DomainMember(config-if)# energywise role role.labphone
DomainMember(config-if)# end

To power off an IP phone connected to a PoE port:

DomainMember# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DomainMember(config)# energywise domain cisco security shared-secret cisco protocol udp port 43440 ip 2.2.4.44
domainMember(config)# interface gigabitethernet0/2
DomainMember(config-if)# energywise importance 65
DomainMember(config-if)# energywise name labphone.5
DomainMember(config-if)# energywise role role.labphone
DomainMember(config-if)# energywise level 0
DomainMember(config-if)# end

The domain member powers the IP phone whether Cisco EnergyWise is enabled or not.

**Examples: Automatically Managing Power**

The following example displays how to automatically manage the power:

DomainMember# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DomainMember(config)# energywise domain cisco security shared-secret cisco protocol udp port 43440 ip 2.2.4.30
domainMember(config)# interface gigabitethernet0/3
DomainMember(config-if)# energywise level 10 recurrence importance 90 at 0 8 * * *
DomainMember(config-if)# energywise level 0 recurrence importance 90 at 0 20 * * *
DomainMember(config-if)# energywise importance 50
DomainMember(config-if)# energywise name labInterface.3
DomainMember(config-if)# energywise role role.labphone
DomainMember(config-if)# end

DomainMember# show energywise recurrences
Id Addr Class Action Lvl Cron
-- ---- ----- ------ --- ----
1 G10/3 QUERY SET 10 minutes: 0 hour: 8 day: * month: * weekday: *
2 G10/3 QUERY SET 0 hour: 20 day: * month: * weekday: *

DomainMember# show running-config
<output truncated>
interface GigabitEthernet0/3
energywise level 10 recurrence at 0 8 * * *
energywise level 0 recurrence at 0 20 *
energywise importance 50
energywise role role.labphone
energywise name labInterface.3
end
<output truncated>
To automatically power on the lab IP phones at 08:00 and power off at 20:00:

```
DomainMember# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DomainMember(config)# energywise domain cisco security shared-secret cisco protocol udp port 43440 ip 2.2.4.30
DomainMember(config)# interface gigabitethernet1/0/3
DomainMember(config-if)# energywise level 10 recurrence importance 90 at 0 8 * * *
DomainMember(config-if)# energywise level 0 recurrence importance 90 at 0 20 * * *
DomainMember(config-if)# energywise importance 50
DomainMember(config-if)# energywise name labInterface.3
DomainMember(config-if)# energywise role role.labphone
DomainMember(config-if)# end
```

```
DomainMember# show energywise recurrences
Id Addr Class Action Lvl Cron
-- ---- ----- ------ --- ----
1 Gi0/3 QUERY SET 10 minutes: 0 hour: 8 day: * month: * weekday: *
2 Gi0/3 QUERY SET 0 minutes: 0 hour: 20: 0 day: * month: * weekday: *
```

```
DomainMember# show running-config
<output truncated>
interface GigabitEthernet0/3
energywise level 10 recurrence importance 70 time-range onfirstfloor
energywise level 0 recurrence at 0 20 *
energywise importance 50
energywise role role.labphone
energywise name floor.1
end
<output truncated>
```

To automatically power on the PCs on the first floor at 06:00 and power off at 21:00:

```
DomainMember# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DomainMember(config)# service password-encryption
DomainMember(config)# energywise domain cisco security shared-secret cisco protocol udp port 43440 ip 2.2.4.30
DomainMember(config)# time-range onfirstfloor
DomainMember(config-time-range)# absolute start 0:00 1 August 2009
DomainMember(config-time-range)# periodic daily 06:00 to 21:00
DomainMember(config)# time-range offfirstfloor
DomainMember(config-time-range)# absolute start 0:00 1 August 2009
DomainMember(config-time-range)# periodic daily 00:00 to 05:55
DomainMember(config-time-range)# periodic daily 21:01 to 23:59
DomainMember(config-time-range)# exit
```

```
DomainMember(config)# interface gigabitethernet0/3
DomainMember(config-if)# energywise level 10 recurrence importance 70 time-range onfirstfloor
DomainMember(config-if)# energywise level 0 recurrence importance 70 time offfirstfloor
DomainMember(config-if)# energywise name floor.1
DomainMember(config-if)# energywise role pc-mgr
DomainMember(config-if)# end
```

```
DomainMember# show energywise recurrences
Id Addr Class Action Lvl Cron
-- ----- ------ ------- --- ----
1 Gi0/3 QUERY SET 10 onfirstfloor
2 Gi0/3 QUERY SET 0 offfirstfloor
```
Examples: Querying to Analyze Domains

This example shows how to display information about the domain, such as the number of members, endpoints and the domain size:

DomainMember# energywise query analyze domain
EnergyWise is currently analyzing the domain, please wait...
EnergyWise Domain Statistics
-----------------------------
Querying from HW Model: WS-C3560G-48PS
Number of Domain Members: 3
Number of Endpoints: 1

Examples: Querying with the Name Attribute

In this example, Switch 1 and Switch 2 are in the same domain. shipping.1 is a PoE port on Switch 1, and shipping.2 is a PoE port on Switch 2.

The example shows the power usage of the domain members and endpoints with names beginning with shipping and with importance values less than or equal to 80. Run this query on Switch 1:

DomainMember# energywise query importance 80 name shipping.* collect usage
EnergyWise query, timeout is 6 seconds:
Host Name Usage Level Imp
----- ----- ------ ----- ---
192.168.20.1 shipping.1 6.3 (W) 10 1
192.168.20.2 shipping.2 8.5 (W) 10 1
Queried: 2 Responded: 2 Time: 0.4 seconds

The first row (shipping.1) is from Switch 1. The second row (shipping.2) is from Switch 2, a neighbor of Switch 1.

Related Topics

Queries, on page 382
Examples: Querying with Keywords

In this example, Switch 1 and Switch 2 are in the same domain. shipping.1 is a PoE port on Switch 1, and shipping.2 is a PoE port on Switch 2.

The example shows the power usage of IP phones with different names, different roles, and importance values less than or equal to 80, but all that have the Admin keyword. Run this query on Switch 1:

```
DomainMember# energywise query importance 80 keyword Admin collect usage
```

```
EnergyWise query, timeout is 6 seconds:
Host Name Usage Level Imp
---- ---- ----- ----- ---
192.168.40.2 shipping.1 6.3 (W) 10 1
192.168.50.2 orders.1 10.3 (W) 10 1
192.168.60.3 pc.1 200.0 (W) 8 75
Queried: 3 Responded: 3 Time: 0.5 seconds
```

Switch 1 reports two phones connected to Switch 2, a neighbor of Switch 1.

---

**Note**

Do not run a query with keywords *. No results are generated.

---

**Related Topics**

Queries, on page 382

Examples: Querying to Set Power Levels

In these examples shipping.1 and shipping.2 are PoE ports on Switch 1. Run these queries on Switch 1:

- Set the power level of PoE port shipping.2 to 0:

```
DomainMember# energywise query importance 80 name shipping.2 set level 0
```

- Set the power level of PoE ports shipping.1 and shipping.2 to 0:

```
DomainMember# energywise query importance 90 name shipping.* set level 0
```

- Set the power level of devices that have the keyword Admin to 10:

```
DomainMember# energywise query importance 60 keyword Admin set level 10
```

```
EnergyWise query, timeout is 6 seconds:
!!!
Success rate is (2/2) setting entities
Queried: 2 Responded: 2 Time: 0.15 seconds
```

To show the power usage of EnergyWise devices with usage type all:

```
DomainMember# energywise query importance 100 name * collect usage all
```

```
EnergyWise query, timeout is 6 seconds:
Host Name Usage Level Imp
---- ---- ----- ----- ---
10.1.2.83 SEP5475d0db0dcb 3.8 (W) 10 5
10.1.2.71 SEP1C17d340834E 8.8 (W) 10 1
10.1.2.68 SEP3037A61748E2 8.8 (W) 10 1
10.1.2.211 Local_InfeedA_Outlet1 0.0 (W) 0 50
```
To show the power usage of an IP phone with usage type **consumer**:

```
DomainMember# energywise query importance 100 name * collect usage consumer
EnergyWise query, timeout is 6 seconds:
Host Name Usage Level Imp
---- ---- ----- ----- ---
10.1.2.83 SEP5475d0db0dcb 3.8 (W) 10 5
10.1.2.71 SEP1C17D340834E 8.8 (W) 10 1
10.1.2.68 SEP3037A61748E2 8.8 (W) 10 1
```

To show the power usage of a PDU outlet with usage type **meter**:

```
DomainMember# energywise query importance 100 name * collect usage meter
EnergyWise query, timeout is 6 seconds:
Host Name Usage Level Imp
---- ---- ----- ----- ---
10.1.2.211 Local_InfeedA_Outlet1 0.0 (W) 0 50
10.1.2.211 Local_InfeedA_Outlet2 0.0 (W) 0 50
10.1.2.211 Local_InfeedA_Outlet3 0.0 (W) 0 50
10.1.2.211 Local_InfeedA_Outlet4 0.0 (W) 0 50
10.1.2.211 Local_InfeedA_Outlet5 0.0 (W) 0 50
10.1.2.211 Local_InfeedA_Outlet6 34.0 (W) 0 50
```

### Related Topics

- **Queries**, on page 382

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnergyWise Commands</td>
<td></td>
</tr>
<tr>
<td>Cisco EnergyWise partner documentation</td>
<td>Go to the Cisco Developer Network.</td>
</tr>
<tr>
<td></td>
<td>- Cisco EnergyWise Documentation Roadmap</td>
</tr>
<tr>
<td></td>
<td>- Cisco EnergyWise Partner Development Guide</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco EnergyWise domain members support the CISCO-ENERGYWISE-MIB.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco IOS MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
PART VIII

QoS

• Configuring QoS, on page 415
Configuring QoS

- Finding Feature Information, on page 415
- Prerequisites for QoS, on page 415
- Restrictions for QoS, on page 416
- Information About QoS, on page 416
- How to Configure QoS, on page 425
- Monitoring Standard QoS, on page 458
- Configuration Examples for QoS, on page 459
- Where to Go Next, on page 467

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for QoS

Before configuring standard QoS, you must have a thorough understanding of these items:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. For example, is the traffic on your network bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

General QoS Guidelines

These are the general QoS guidelines:
• Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch are subject to all ingress QoS processing.

• You are likely to lose data when you change queue settings; therefore, try to make changes when traffic is at a minimum.

Restrictions for QoS

The following are the restrictions for QoS:

• The switch does not support classifying of traffic using class maps (class-map global configuration command).

• Ingress queueing is not supported.

• Interface restrictions:
  • Enable only cos trust at interface level.
  • Enable SRR shaping and sharing at interface level.
  • Enable Priority queueing at interface level.

Information About QoS

QoS Implementation

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, a standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.
Layer 2 Frame Prioritization Bits

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

Other frame types cannot carry Layer 2 CoS values.

Layer 2 CoS values range from 0 for low priority to 7 for high priority.

Layer 3 Packet Prioritization Bits

Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.

IP precedence values range from 0 to 7. DSCP values range from 0 to 63.
QoS Basic Model

To implement QoS, the switch must distinguish packets or flows from one another (classify), assign a label to indicate the given quality of service as the packets move through the switch, make the packets comply with the configured resource usage limits (police and mark), and provide different treatment (queue and schedule) in all situations where resource contention exists. The switch also needs to ensure that traffic sent from it meets a specific traffic profile (shape).

Figure 39: QoS Basic Wired Model

Actions at Ingress Port

Actions at the ingress port include classifying traffic, policing, marking, and scheduling:

- Classifying a distinct path for a packet by associating it with a QoS label. The switch maps the CoS or DSCP in the packet to a QoS label to distinguish one kind of traffic from another. The QoS label that is generated identifies all future QoS actions to be performed on this packet.

- Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.

- Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, marking down the QoS label in the packet, or dropping the packet).

Note: Queueing and scheduling are only supported at egress and not at ingress on the switch.

Actions at Egress Port

Actions at the egress port include queueing and scheduling:

- Queueing evaluates the QoS packet label and the corresponding DSCP or CoS value before selecting which of the four egress queues to use. Because congestion can occur when multiple ingress ports simultaneously send data to an egress port, WTD differentiates traffic classes and subjects the packets to different thresholds based on the QoS label. If the threshold is exceeded, the packet is dropped.

- Scheduling services the four egress queues based on their configured SRR shared or shaped weights. One of the queues (queue 1) can be the priority queue, which is serviced until empty before the other queues are serviced.
Mapping Tables Overview

During QoS processing, the switch represents the priority of all traffic (including non-IP traffic) with a QoS label based on the DSCP or CoS value from the classification stage.

The following table describes QoS processing and mapping tables.

<table>
<thead>
<tr>
<th>QoS Processing Stage</th>
<th>Mapping Table Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classification</strong></td>
<td>During the classification stage, QoS uses configurable mapping tables to derive a corresponding DSCP or CoS value from a received CoS, DSCP, or IP precedence value. These maps include the CoS-to-DSCP map and the IP-precedence-to-DSCP map. You configure these maps by using the <code>mls qos map cos-dscp</code> and the <code>mls qos map ip-prec-dscp</code> global configuration commands. On an ingress port configured in the DSCP-trusted state, if the DSCP values are different between the QoS domains, you can apply the configurable DSCP-to-DSCP-mutation map to the port that is on the boundary between the two QoS domains. You configure this map by using the <code>mls qos map dscp-mutation</code> global configuration command.</td>
</tr>
<tr>
<td><strong>Policing</strong></td>
<td>During policing stage, QoS can assign another DSCP value to an IP or a non-IP packet (if the packet is out of profile and the policer specifies a marked-down value). This configurable map is called the policed-DSCP map. You configure this map by using the <code>mls qos map policed-dscp</code> global configuration command.</td>
</tr>
<tr>
<td><strong>Pre-scheduling</strong></td>
<td>Before the traffic reaches the scheduling stage, QoS stores the packet in an egress queue according to the QoS label. The QoS label is based on the DSCP or the CoS value in the packet and selects the queue through the DSCP output queue threshold maps or through the CoS output queue threshold maps. In addition to an egress queue, the QOS label also identifies the WTD threshold value. You configure these maps by using the <code>mls qos srr-queue {output} dscp-map</code> and the <code>mls qos srr-queue {output} cos-map</code> global configuration commands.</td>
</tr>
</tbody>
</table>

The CoS-to-DSCP, DSCP-to-CoS, and the IP-precedence-to-DSCP maps have default values that might or might not be appropriate for your network.

The default DSCP-to-DSCP-mutation map and the default policed-DSCP map are null maps; they map an incoming DSCP value to the same DSCP value. The DSCP-to-DSCP-mutation map is the only map you apply to a specific port. All other maps apply to the entire switch.

**Related Topics**

- Configuring DSCP Maps
- Queueing and Scheduling on Egress Queues
Queueing and Scheduling Overview

The switch has queues at specific points to help prevent congestion.

*Figure 40: Egress Queue Location on Switch*

The switch supports 4 egress queues by default and there is an option to enable a total of 8 egress queues. The 8 egress queue configuration is only supported on a standalone switch.

The Catalyst 2960-L switches support Scheduled Round Robin (SRR). They do not support Weighted Round Robin (WRR). Currently, you can configure SRR with `wrr` commands instead of `srr` commands. From Cisco IOS Release 15.2(5)E2 and later, the `wrr` commands will be replaced with the `srr` commands on the switch.

Queueing and Scheduling on Egress Queues

The following figure shows queueing and scheduling flowcharts for egress ports on the switch.
Figure 41: Queueing and Scheduling Flowchart for Egress Ports on the Switch

1. Start
2. Receive packet from the stack ring.
3. Read QoS label (DSCP or CoS value).
4. Determine egress queue number and threshold based on the label.
5. Are thresholds being exceeded?
   - Yes: Drop packet.
   - No: Queue the packet. Service the queue according to the SRR weights.
6. Rewrite DSCP and/or CoS value as appropriate.
7. Send the packet out the port.
8. Done

Note
If the priority queue is enabled, SRR services it until it is empty before servicing the other three queues.

Egress Expedite Queue

Each port supports four egress queues, one of which (queue 1) can be the egress expedite queue. These queues are assigned to a queue-set. All traffic exiting the switch flows through one of these four queues and is subjected to a threshold based on the QoS label assigned to the packet.
If the expedite queue is enabled, SRR services it until it is empty before servicing the other three queues.

### Egress Queue Buffer Allocation

The following figure shows the egress queue buffer.

*Figure 42: Egress Queue Buffer Allocation*

The buffer space is divided between the common pool and the reserved pool. The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to control whether to grant buffer space to a requesting queue. The switch detects whether the target queue has not consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over limit), and whether the common pool is empty (no free buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

### Buffer and Memory Allocation

You guarantee the availability of buffers, set drop thresholds, and configure the maximum memory allocation for a queue-set by using the `mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` global configuration command. Each threshold value is a percentage of the queue’s allocated memory, which you specify by using the `mls qos queue-set output qset-id buffers allocation1 ... allocation4` global configuration command. The sum of all the allocated buffers represents the reserved pool, and the remaining buffers are part of the common pool.

Through buffer allocation, you can ensure that high-priority traffic is buffered. For example, if the buffer space is 400, you can allocate 70 percent of it to queue 1 and 10 percent to queues 2 through 4. Queue 1 then has 280 buffers allocated to it, and queues 2 through 4 each have 40 buffers allocated to them.

You can guarantee that the allocated buffers are reserved for a specific queue in a queue-set. For example, if there are 100 buffers for a queue, you can reserve 50 percent (50 buffers). The switch returns the remaining 50 buffers to the common pool. You also can enable a queue in the full condition to obtain more buffers than are reserved for it by setting a maximum threshold. The switch can allocate the needed buffers from the common pool if the common pool is not empty.
Queues and WTD Thresholds

You can assign each packet that flows through the switch to a queue and to a threshold. Specifically, you map DSCP or CoS values to an egress queue and map DSCP or CoS values to a threshold ID. You use the `mls qos srr-queue output dscp-map queue queue-id | threshold threshold-id | cos1...cos8 | threshold threshold-id cos1...cos8` or the `mls qos srr-queue output cos-map queue queue-id | threshold threshold-id cos1...cos8 | threshold threshold-id cos1...cos8` global configuration command. You can display the DSCP output queue threshold map and the CoS output queue threshold map by using the `show mls qos maps` privileged EXEC command.

The queues use WTD to support distinct drop percentages for different traffic classes. Each queue has three drop thresholds: two configurable (explicit) WTD thresholds and one nonconfigurable (implicit) threshold preset to the queue-full state. You assign the two WTD threshold percentages for threshold ID 1 and ID 2. The drop threshold for threshold ID 3 is preset to the queue-full state, and you cannot modify it. You map a port to queue-set by using the `queue-set qset-id` interface configuration command. Modify the queue-set configuration to change the WTD threshold percentages.

Note

The switch supports 4 egress queues by default, although there is an option to enable a total of 8 egress queues. Use the `mls qos srr-queue output queues 8` global configuration command to enable all 8 egress queues. Once 8 egress queues are enabled, you are able to configure thresholds and buffers for all 8 queues. The 8 egress queue configuration is only supported on a standalone switch.

Related Topics

Weighted Tail Drop

Shaped or Shared Mode

SRR services each queue-set in shared or shaped mode. You map a port to a queue-set by using the `queue-set qset-id` interface configuration command. You assign shared or shaped weights to the port by using the `srr-queue bandwidth share weight1 weight2 weight3 weight4` or the `srr-queue bandwidth shape weight1 weight2 weight3 weight4` interface configuration command.

The buffer allocation together with the SRR weight ratios control how much data can be buffered and sent before packets are dropped. The weight ratio is the ratio of the frequency in which the SRR scheduler sends packets from each queue.

All four queues participate in the SRR unless the expedite queue is enabled, in which case the first bandwidth weight is ignored and is not used in the ratio calculation. The expedite queue is a priority queue, and it is serviced until empty before the other queues are serviced. You enable the expedite queue by using the `priority-queue out` interface configuration command.

You can combine the commands described in this section to prioritize traffic by placing packets with particular CoSs into certain queues, by allocating a large queue size or by servicing the queue more frequently, and by adjusting queue thresholds so that packets with lower priorities are dropped.

Note

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Related Topics

Configuring Egress Queue Characteristics, on page 447
SRR Shaping and Sharing
Packet Modification

A packet is classified and queued to provide QoS. The following packet modifications can occur during the process to provide QoS:

- For IP and non-IP packets, classification involves assigning a QoS label to a packet based on the CoS of the received packet. However, the packet is not modified at this stage; only an indication of the assigned CoS value is carried along.
- If you configure the port to trust the CoS of the incoming frame and it is an IP packet, the CoS value in the frame is not changed.

Standard QoS Default Configuration

QoS is disabled by default.

When QoS is disabled, there is no concept of trusted or untrusted ports because the packets are not modified. The CoS, DSCP, and IP precedence values in the packet are not changed.

Traffic is switched in pass-through mode. The packets are switched without any rewrites and classified as best effort without any policing.

When QoS is enabled using the mls qos global configuration command and all other QoS settings are at their defaults, traffic is classified as best effort (the DSCP and CoS value is set to 0) without any policing. No policy maps are configured. The default port trust state on all ports is untrusted.

Related Topics
- Enabling QoS Globally, on page 425
- Default Egress Queue Configuration, on page 424

Default Egress Queue Configuration

The following tables describe the default egress queue configurations.

The following table shows the default egress queue configuration for each queue-set when QoS is enabled. All ports are mapped to queue-set 1. The port bandwidth limit is set to 100 percent and rate unlimited. Note that for the SRR shaped weights (absolute) feature, a shaped weight of zero indicates that the queue is operating in shared mode. Note that for the SRR shared weights feature, one quarter of the bandwidth is allocated to each queue.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Queue 1</th>
<th>Queue 2</th>
<th>Queue 3</th>
<th>Queue 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer allocation</td>
<td>25 percent</td>
<td>25 percent</td>
<td>25 percent</td>
<td>25 percent</td>
</tr>
<tr>
<td>WTD drop threshold 1</td>
<td>100 percent</td>
<td>200 percent</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>WTD drop threshold 2</td>
<td>100 percent</td>
<td>200 percent</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>Reserved threshold</td>
<td>50 percent</td>
<td>50 percent</td>
<td>50 percent</td>
<td>50 percent</td>
</tr>
<tr>
<td>Maximum threshold</td>
<td>400 percent</td>
<td>400 percent</td>
<td>400 percent</td>
<td>400 percent</td>
</tr>
</tbody>
</table>
The following table shows the default CoS output queue threshold map when QoS is enabled.

### Table 56: Default CoS Output Queue Threshold Map

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 1</td>
<td>2–1</td>
</tr>
<tr>
<td>2, 3</td>
<td>3–1</td>
</tr>
<tr>
<td>4</td>
<td>4–1</td>
</tr>
<tr>
<td>5</td>
<td>1–1</td>
</tr>
<tr>
<td>6, 7</td>
<td>4–1</td>
</tr>
</tbody>
</table>

**Related Topics**
- Enabling QoS Globally, on page 425
- Standard QoS Default Configuration, on page 424

### Default Mapping Table Configuration

The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value (no markdown).

**Related Topics**
- Default CoS-to-DSCP Map
- Default IP-Precedence-to-DSCP Map
- Default DSCP-to-CoS Map

## How to Configure QoS

### Enabling QoS Globally

By default, QoS is disabled on the switch.

The following procedure to enable QoS globally is required.

**SUMMARY STEPS**

1. `configure terminal`
2. mls qos  
3. end  
4. show mls qos  
5. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> mls qos</td>
<td>Enables QoS globally. QoS operates with the default settings described in the related topic sections below.</td>
</tr>
<tr>
<td>Example: Switch(config)# mls qos</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show mls qos</td>
<td>Verifies the QoS configuration.</td>
</tr>
<tr>
<td>Example: Switch# show mls qos</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Standard QoS Default Configuration, on page 424
- Default Egress Queue Configuration, on page 424

### Enabling VLAN-Based QoS on Physical Ports

By default, VLAN-based QoS is disabled on all physical switch ports. You can enable VLAN-based QoS on a switch port.
SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. mls qos vlan-based
4. end
5. show mls qos interface interface-id
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode. |
| Step 2 | interface interface-id  
Example:  
Switch(config)# interface gigabitethernet 1/0/1 | Specifies the physical port, and enter interface configuration mode. |
| Step 3 | mls qos vlan-based  
Example:  
Switch(config-if)# mls qos vlan-based | Enables VLAN-based QoS on the port.  
Note: Use the no mls qos vlan-based interface configuration command to disable VLAN-based QoS on the physical port. |
| Step 4 | end  
Example:  
Switch(config-if)# end | Returns to privileged EXEC mode. |
| Step 5 | show mls qos interface interface-id  
Example:  
Switch# show mls qos interface gigabitethernet 1/0/1 | Verifies if VLAN-based QoS is enabled on the physical port. |
| Step 6 | copy running-config startup-config  
Example:  
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
Configuring a QoS Policy

Configuring a QoS policy typically requires the following tasks:

• Classifying traffic into classes
• Configuring policies applied to those traffic classes
• Attaching policies to ports

These sections describe how to classify, police, and mark traffic. Depending on your network configuration, you must perform one or more of the modules in this section.

Related Topics
Policing and Marking Overview
Classification Overview

Classifying Traffic by Using ACLs

You can classify IP traffic by using IPv4 standard ACLs, IPv4 extended ACLs, or IPv6 ACLs.
You can classify non-IP traffic by using Layer 2 MAC ACLs.

Creating an IP Standard ACL for IPv4 Traffic

Before you begin
Before you perform this task, determine which access lists you will be using for your QoS configuration.

SUMMARY STEPS

1. configure terminal
2. access-list access-list-number {deny | permit} source [source-wildcard]
3. end
4. show access-lists
5. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Creates an IP standard ACL, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td>access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# access-list 1</td>
<td>• For access-list-number, enter the access list number. The range is 1 to 99 and 1300 to 1999.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| permit 192.2.255.0 1.1.1.255 | • Use the **permit** keyword to permit a certain type of traffic if the conditions are matched. Use the **deny** keyword to deny a certain type of traffic if conditions are matched.  
• For **source**, enter the network or host from which the packet is being sent. You can use the **any** keyword as an abbreviation for 0.0.0.0–255.255.255.255.  
• (Optional) For **source-wildcard**, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.  
When you create an access list, remember that by default the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end. |

**Step 3**

**Example:**

Switch(config)# **end**

Returns to privileged EXEC mode.

**Step 4**

**Example:**

Switch# **show access-lists**

Verifies your entries.

**Step 5**

**Example:**

Switch# **copy running-config startup-config**

(Optional) Saves your entries in the configuration file.

**Related Topics**

Access Control Lists  
QoS ACL Guidelines  
Examples: Classifying Traffic by Using ACLs, on page 459
Creating an IP Extended ACL for IPv4 Traffic

Before you begin

Before you perform this task, determine which access lists you will be using for your QoS configuration.

SUMMARY STEPS

1. `configure terminal`
2. `access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard`
3. `end`
4. `show access-lists`
5. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Example:

```
Switch# configure terminal
```

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>Creates an IP extended ACL, repeating the command as many times as necessary.</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list access-list-number {deny</td>
<td>permit} protocol source source-wildcard destination destination-wildcard</td>
</tr>
</tbody>
</table>

Example:

```
Switch(config)# access-list 100 permit ip any any dscp 32
```
For destination, enter the network or host to which the packet is being sent. You have the same options for specifying the destination and destination-wildcard as those described by source and source-wildcard.

When creating an access list, remember that, by default, the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

**Note** To delete an access list, use the no access-list access-list-number global configuration command.

**Step 3**

**Command or Action**

**Purpose**

- For destination, enter the network or host to which the packet is being sent. You have the same options for specifying the destination and destination-wildcard as those described by source and source-wildcard.

**Step 4**

**Command or Action**

**Purpose**

- Returns to privileged EXEC mode.

**Step 5**

**Related Topics**

- Access Control Lists
- QoS ACL Guidelines
- Examples: Classifying Traffic by Using ACLs, on page 459

Creating an IPv6 ACL for IPv6 Traffic

**Before you begin**

Before you perform this task, determine which access lists you will be using for your QoS configuration.

**SUMMARY STEPS**

1. configure terminal
2. ipv6 access-list access-list-name
3. \{deny | permit\} protocol \{source-ipv6-prefix/prefix-length | any | host source-ipv6-address\} \{operator [port-number]\} \{destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address\} \{operator [port-number]\} \{dscp value | fragments | log | log-input | routing | sequence value | time-range name\}
Creating an IPv6 ACL for IPv6 Traffic

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>ipv6 access-list access-list-name</td>
<td>Creates an IPv6 ACL and enters IPv6 access-list configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 access-list ipv6_Name_ACL</td>
<td>Accesses list names cannot contain a space or quotation mark or begin with a numeric.</td>
</tr>
</tbody>
</table>

**Note** To delete an access list, use the **no ipv6 access-list access-list-number** global configuration command.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>[deny</td>
<td>permit] protocol [source-ipv6-prefix/prefix-length</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-ipv6-acl)# permit ip host 10::1 host 11::2 host</td>
<td>For protocol, enter the name or number of an Internet protocol: <strong>ahp</strong>, <strong>esp</strong>, <strong>icmp</strong>, <strong>ipv6</strong>, <strong>pcp</strong>, <strong>stcp</strong>, <strong>tcp</strong>, or <strong>udp</strong>, or an integer in the range 0 to 255 representing an IPv6 protocol number.</td>
</tr>
</tbody>
</table>

- The **source-ipv6-prefix/prefix-length** or **destination-ipv6-prefix/ prefix-length** is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373).
- Enter **any** as an abbreviation for the IPv6 prefix ::/0.
- For **host source-ipv6-address** or **destination-ipv6-address**, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons.
- (Optional) For **operator**, specify an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range**.

If the operator follows the **source-ipv6-prefix/prefix-length** argument, it must...
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>match the source port. If the operator follows the destination-ipv6-prefix/prefix-length argument, it must match the destination port.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) The port-number is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter dscp value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter fragments to check noninitial fragments. This keyword is visible only if the protocol is IPv6.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter log to cause a logging message to be sent to the console about the packet that matches the entry. Enter log-input to include the input interface in the log entry. Logging is supported only for router ACLs.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter routing to specify that IPv6 packets be routed.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter sequence value to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter time-range name to specify the time range that applies to the deny or permit statement.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**

**Example:**
```
Switch(config-ipv6-acl)# end
```

Returns to privileged EXEC mode.

**Step 5**

**show ipv6 access-list**

**Example:**
```
Switch# show ipv6 access-list
```

Verifies the access list configuration.

**Step 6**

**copy running-config startup-config**

**Example:**
```
Switch# copy running-config
```

(Optional) Saves your entries in the configuration file.
Creating a Layer 2 MAC ACL for Non-IP Traffic

**Before you begin**

Before you perform this task, determine that Layer 2 MAC access lists are required for your QoS configuration.

**SUMMARY STEPS**

1. **configure terminal**
2. **mac access-list extended** name
3. `{permit | deny} {host src-MAC-addr mask | any | host dst-MAC-addr | dst-MAC-addr mask} [type mask]
4. **end**
5. **show access-lists** [access-list-number | access-list-name]
6. **copy running-config startup-config**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| configure terminal |
| Example:
| `Switch# configure terminal` |
| **Step 2**
| mac access-list extended name |
| Example:
| `Switch(config)# mac access-list extended maclist1` |
| **Step 3**
| `{permit | deny} {host src-MAC-addr mask | any | host dst-MAC-addr | dst-MAC-addr mask} [type mask]` |
| Example:
| `Switch(config-ext-mac1) # permit 0001.0000.0001` |

**Related Topics**

- Access Control Lists
- QoS ACL Guidelines
- Examples: Classifying Traffic by Using ACLs, on page 459
- QoS ACL IPv6 Guidelines
### Command or Action

<table>
<thead>
<tr>
<th></th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0 0002.0000.0001 0.0.0</td>
<td>by using the hexadecimal format (H.H.H), by using the <em>any</em> keyword as an abbreviation for <em>source</em> 0.0.0, <em>source-wildcard</em> ffff.ffff.ffff, or by using the <em>host</em> keyword for <em>source</em> 0.0.0.</td>
</tr>
</tbody>
</table>
| 0.0.0 0002.0000.0002 0.0.0 xns-idp | • For *mask*, enter the wildcard bits by placing ones in the bit positions that you want to ignore.  
• For *dst-MAC-addr*, enter the MAC address of the host to which the packet is being sent. You specify this by using the hexadecimal format (H.H.H), by using the *any* keyword as an abbreviation for *source* 0.0.0, *source-wildcard* ffff.ffff.ffff, or by using the *host* keyword for *source* 0.0.0.  
• (Optional) For *type mask*, specify the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. For *type*, the range is from 0 to 65535, typically specified in hexadecimal. For *mask*, enter the *don’t care* bits applied to the Ethertype before testing for a match. |

### Step 4

**end**

**Example:**

```
Switch(config-ext-macl) # end
```

Returns to privileged EXEC mode.

### Step 5

**show access-lists [access-list-number | access-list-name]**

**Example:**

```
Switch# show access-lists
```

Verifies your entries.

### Step 6

**copy running-config startup-config**

**Example:**

```
Switch# copy-running-config startup-config
```

(Optional) Saves your entries in the configuration file.

---

**Related Topics**

- Access Control Lists
- QoS ACL Guidelines
- Examples: Classifying Traffic by Using ACLs, on page 459
Classifying Traffic by Using Class Maps

You use the class-map global configuration command to name and to isolate a specific traffic flow (or class) from all other traffic. The class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as an ACL, IP precedence values, or DSCP values. The match criterion is defined with one match statement entered within the class-map configuration mode.

**Summary Steps**

1. `configure terminal`
2. Use one of the following:
   - `access-list access-list-number {deny | permit} source [source-wildcard]`
   - `access-list access-list-number {deny | permit} protocol source [source-wildcard] destination [destination-wildcard]`
   - `ipv6 access-list access-list-name {deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/ prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence value] [time-range name]`
   - `mac access-list extended name {permit | deny} {host src-MAC-addr mask | any | host dst-MAC-addr | dst-MAC-addr mask} [type mask]`
3. `class-map [match-all | match-any] class-map-name`
4. `match {access-group acl-index-or-name | ip dscp dscp-list | ip precedence ip-precedence-list}`
5. `end`
6. `show class-map`
7. `copy running-config startup-config`

**Detailed Steps**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 Use one of the following:</td>
<td>Creates an IP standard or extended ACL, an IPv6 ACL for IP traffic, or a Layer 2 MAC ACL for non-IP traffic, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td>• `access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]`</td>
</tr>
<tr>
<td>• `access-list access-list-number {deny</td>
<td>permit} protocol source [source-wildcard] destination [destination-wildcard]`</td>
</tr>
<tr>
<td>• `ipv6 access-list access-list-name {deny</td>
<td>permit} protocol {source-ipv6-prefix/prefix-length</td>
</tr>
</tbody>
</table>
### QoS

#### Classifying Traffic by Using Class Maps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>source-ipv6-address} [operator [port-number]]</code></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>`{destination-ipv6-prefix/ prefix-length</td>
<td>any</td>
</tr>
<tr>
<td><code>destination-ipv6-address} [operator [port-number]]</code></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>[dscp value] [fragments] [log] [log-input] [routing]</code></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>[sequence value] [time-range name]</code></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>• `mac access-list extended name {permit</td>
<td>deny}</td>
</tr>
<tr>
<td>`src-MAC-addr mask</td>
<td>any</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config)# access-list 103 permit ip any any dscp 10
```

**Step 3**

```
class-map [match-all | match-any] class-map-name
```

**Example:**

```
Switch(config)# class-map class1
```

**Step 4**

```
match {access-group acl-index-or-name | ip dscp dscp-list |
| ip precedence ip-precedence-list} `Create a class map, and enters class-map configuration mode.

By default, no class maps are defined.

• (Optional) Use the **match-all** keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched.

• (Optional) Use the **match-any** keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched.

• For **class-map-name**, specify the name of the class map.

If neither the **match-all** or **match-any** keyword is specified, the default is **match-all**.

**Note** To delete an existing class map, use the no **class-map [match-all | match-any] class-map-name** global configuration command.

**Example:**

```
Switch(config-cmap)# match ip dscp 10 11 12
```

**Purpose**

**Define the match criterion to classify traffic.**

By default, no match criterion is defined.

Only one match criterion per class map is supported, and only one ACL per class map is supported.

• For **access-group acl-index-or-name**, specify the number or name of the ACL created in Step 2.

• To filter IPv6 traffic with the **match access-group** command, create an IPv6 ACL, as described in Step 2.

• For **ip dscp dscp-list**, enter a list of up to eight IP DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63.
Classifying Traffic by Using Class Maps and Filtering IPv6 Traffic

**SUMMARY STEPS**

1. configure terminal
2. class-map {match-all} class-map-name
3. match protocol [ip | ipv6]
4. match {ip dscp dscp-list | ip precedence ip-precedence-list}

IPv6 QoS is not supported on switches running the LAN base feature set.

To apply the primary match criteria to only IPv4 traffic, use the `match protocol` command with the `ip` keyword. To apply the primary match criteria to only IPv6 traffic, use the `match protocol` command with the `ipv6` keyword.

**Related Topics**
- Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps, on page 440
- Classifying, Policing, and Marking Traffic on SVIs by Using Hierarchical Policy Maps
- Examples: Classifying Traffic by Using Class Maps, on page 460
5. end
6. show class-map
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> class-map [match-all] class-map-name</td>
<td>Creates a class map, and enters class-map configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# class-map cm-1</td>
<td>By default, no class maps are defined.</td>
</tr>
<tr>
<td></td>
<td>When you use the match protocol command, only the match-all keyword is supported.</td>
</tr>
<tr>
<td></td>
<td>• For class-map-name, specify the name of the class map.</td>
</tr>
<tr>
<td></td>
<td>If neither the match-all or match-any keyword is specified, the default is match-all.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To delete an existing class map, use the no class-map [match-all</td>
</tr>
<tr>
<td><strong>Step 3</strong> match protocol [ip</td>
<td>ipv6]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-cmap)# match protocol ip</td>
<td>• Use the argument ip to specify IPv4 traffic and ipv6 to specify IPv6 traffic.</td>
</tr>
<tr>
<td></td>
<td>• When you use the match protocol command, only the match-all keyword is supported for the class-map command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> match [ip dscp dscp-list</td>
<td>ip precedence</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-cmap)# match ip dscp 10</td>
<td>By default, no match criterion is defined.</td>
</tr>
<tr>
<td></td>
<td>• For ip dscp dscp-list, enter a list of up to eight IP DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63.</td>
</tr>
<tr>
<td></td>
<td>• For ip precedence ip-precedence-list, enter a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Toremoveamatchcriterion,usethenomatch\{access-group acl-index-or-name | To remove a match criterion, use the no match
| | \( ip\ dscp \) | class-map configuration command. |

### Note

ReturnstoprivilegedEXECmode.

### Step 5

**Example:**

```
Switch(config-cmap)# end
```

### Step 6

**Example:**

```
Switch# show class-map
```

### Step 7

**Example:**

```
Switch# copy-running-config startup-config
```

### Related Topics

Examples: Classifying Traffic by Using Class Maps, on page 460

---

**Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps**

You can configure a policy map on a physical port that specifies which traffic class to act on. Actions can include trusting the CoS, DSCP, or IP precedence values in the traffic class; setting a specific DSCP or IP precedence value in the traffic class; and specifying the traffic bandwidth limitations for each matched traffic class (policer) and the action to take when the traffic is out of profile (marking).

A policy map also has these characteristics:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.
- A separate policy-map class can exist for each type of traffic received through a port.

Follow these guidelines when configuring policy maps on physical ports:

- You can attach only one policy map per ingress port.
- If you configure the IP-precedence-to-DSCP map by using the `mls qos map ip-prec-dscp` global configuration command, the settings only affect packets on ingress interfaces that are configured to trust the IP precedence value. In a policy map, if you set the packet IP precedence value to a new value by using the `set ip precedence new-precedence` policy-map class configuration command, the egress DSCP value is not affected by the IP-precedence-to-DSCP map. If you want the egress DSCP value to be different than the ingress value, use the `set dscp new-dscp` policy-map class configuration command.
• If you enter or have used the `set ip dscp` command, the switch changes this command to `set dscp` in its configuration.

• You can use the `set ip precedence` or the `set precedence` policy-map class configuration command to change the packet IP precedence value. This setting appears as set ip precedence in the switch configuration.

• A policy-map and a port trust state can both run on a physical interface. The policy-map is applied before the port trust state.

• When you configure a default traffic class by using the `class class-default` policy-map configuration command, unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as the default traffic class (class-default).

**SUMMARY STEPS**

1. configure terminal
2. class-map [match-all | match-any] class-map-name
3. policy-map policy-map-name
4. class [class-map-name | class-default]
5. trust [cos | dscp | ip-precedence]
6. set {dscp new-dscp | ip precedence new-precedence}
7. police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]
8. exit
9. exit
10. interface interface-id
11. service-policy input policy-map-name
12. end
13. show policy-map [policy-map-name [class class-map-name]]
14. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Creates a class map, and enters class-map configuration mode. |
| class-map [match-all | match-any] class-map-name | By default, no class maps are defined. |
| **Example:** | |
| Switch(config)# class-map ipclass1 | |

- (Optional) Use the `match-all` keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• (Optional) Use the <strong>match-any</strong> keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched.</td>
<td></td>
</tr>
<tr>
<td>• For <strong>class-map-name</strong> , specify the name of the class map.</td>
<td></td>
</tr>
<tr>
<td>If neither the <strong>match-all</strong> or <strong>match-any</strong> keyword is specified, the default is <strong>match-all</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

**policy-map** *policy-map-name*

**Example:**

```
Switch(config-cmap)# policy-map flowit
```

Creates a policy map by entering the policy map name, and enters policy-map configuration mode.

By default, no policy maps are defined.

The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed.

**Note** To delete an existing policy map, use the **no policy-map** *policy-map-name* global configuration command.

**Step 4**

**class** [*class-map-name | class-default*]

**Example:**

```
Switch(config-pmap)# class ipclass1
```

Defines a traffic classification, and enters policy-map class configuration mode.

By default, no policy map class-maps are defined.

If a traffic class has already been defined by using the **class-map** global configuration command, specify its name for **class-map-name** in this command.

A **class-default** traffic class is pre-defined and can be added to any policy. It is always placed at the end of a policy map. With an implied **match any** included in the **class-default** class, all packets that have not already matched the other traffic classes will match **class-default**.

**Note** To delete an existing class map, use the **no class** *class-map-name* policy-map configuration command.

**Step 5**

**trust** [*cos | dscp | ip-precedence*]

**Example:**

```
Switch(config-pmap-c)# trust dscp
```

Configures the trust state, which QoS uses to generate a CoS-based or DSCP-based QoS label.

This command is mutually exclusive with the **set** command within the same policy map. If you enter the **trust** command, go to Step 6.

By default, the port is not trusted. If no keyword is specified when the command is entered, the default is **dscp**.

The keywords have these meanings:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>cos</strong>—QoS derives the DSCP value by using the received or default port CoS value and the CoS-to-DSCP map.</td>
<td></td>
</tr>
<tr>
<td>• <strong>dscp</strong>—QoS derives the DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the default port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.</td>
<td></td>
</tr>
<tr>
<td>• <strong>ip-precedence</strong>—QoS derives the DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the default port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  
To return to the untrusted state, use the **no trust** policy-map configuration command.

**Step 6**  
**set** {**dscp new-dscp** | **ip precedence new-precedence**}  
**Example:**  
Switch(config-pmap-c)# set dscp 45

**Step 7**  
**police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]**  
**Example:**  
Switch(config-pmap-c)# police 100000 80000 drop

**Classifies IP traffic by setting a new value in the packet.**  
- For **dscp new-dscp**, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63.  
- For **ip precedence new-precedence**, enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7.

**Note**  
To remove an assigned DSCP or IP precedence value, use the **no set** {**dscp new-dscp** | **ip precedence new-precedence**} policy-map configuration command.

**Defines a policer for the classified traffic.**  
By default, no policer is defined.  
- For **rate-bps**, specify average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.  
- For **burst-byte**, specify the normal burst size in bytes. The range is 8000 to 1000000.  
- (Optional) Specifies the action to take when the rates are exceeded. Use the **exceed-action drop** keywords to drop the packet. Use the **exceed-action policed-dscp-transmit** keywords to mark down the...
## QoS

### Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP value (by using the policed-DSCP map) and to send the packet. <strong>Note</strong> To remove an existing policer, use the **no police rate-bps burst-byte [exceed-action {drop</td>
<td>policed-dscp-transmit}]** policy-map configuration command.</td>
</tr>
</tbody>
</table>

**Step 8**

exit

**Example:**

Switch(config-pmap-c)# exit

**Step 9**

exit

**Example:**

Switch(config-pmap)# exit

**Step 10**

interface interface-id

**Example:**

Switch(config)# interface gigabitethernet 2/0/1

**Step 11**

service-policy input policy-map-name

**Example:**

Switch(config-if)# service-policy input flowit

**Step 12**

end

**Example:**

Switch(config-if)# end

**Step 13**

show policy-map [policy-map-name [class class-map-name]]

**Example:**

Switch# show policy-map

Verifies your entries.
### Purpose

Command or Action | Purpose
--- | ---
Step 14 | copy running-config startup-config

(Optional) Saves your entries in the configuration file.

#### Example:

| Switch# | copy-running-config startup-config |

---

### Related Topics

- Policing and Marking Overview
- Physical Port Policing
- Classifying Traffic by Using Class Maps, on page 436
- Policy Map on Physical Port
- Examples: Classifying, Policing, and Marking Traffic on Physical Ports Using Policy Maps, on page 462
- Policy Map on Physical Port Guidelines

---

### Classifying, Policing, and Marking Traffic by Using Aggregate Policers

By using an aggregate policer, you can create a policer that is shared by multiple traffic classes within the same policy map. However, you cannot use the aggregate policer across different policy maps or ports.

You can configure aggregate policers only in nonhierarchical policy maps on physical ports.

### SUMMARY STEPS

1. configure terminal
2. mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action \{drop | policed-dscp-transmit\}
3. class-map [match-all | match-any] class-map-name
4. policy-map policy-map-name
5. class [class-map-name | class-default]
6. police aggregate aggregate-policer-name
7. exit
8. interface interface-id
9. service-policy input policy-map-name
10. end
11. show mls qos aggregate-policer [aggregate-policer-name]
12. copy running-config startup-config

---

### DETAILED STEPS

| Command or Action | Purpose |
--- | ---
Step 1 | configure terminal

Enters global configuration mode.

| Switch# | configure terminal |

---

### Command or Action

| Command or Action | Purpose |
--- | ---
Step 1 | configure terminal

Example:

| Switch# | configure terminal |

---
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>`mls qos aggregate-police aggregate-policer-name rate-bps burst-byte exceed-action {drop</td>
<td>policed-dscp-transmit}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action policed-dscp-transmit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`class-map [match-all</td>
<td>match-any] class-map-name`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# class-map ipclass1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>policy-map policy-map-name</code></td>
<td>Creates a policy map by entering the policy map name, and enters policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-cmap)# policy-map aggflow1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`class [class-map-name</td>
<td>class-default]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-cmap-p)# class ipclass1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>police aggregate aggregate-policer-name</code></td>
<td>Applies an aggregate policer to multiple classes in the same policy map. For <code>aggregate-policer-name</code>, enter the name specified in Step 2.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(configure-cmap-p)# police aggregate transmit1</code></td>
<td>To remove the specified aggregate policer from a policy map, use the <code>no police aggregate aggregate-policer-name</code> policy map configuration command. To delete an aggregate policer and its parameters, use the <code>no mls qos aggregate-police aggregate-policer-name</code> global configuration command.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(configure-cmap-p)# exit</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>interface interface-id</td>
<td>Specifies the port to attach to the policy map, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 2/0/1</td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td>9</td>
<td>service-policy input policy-map-name</td>
<td>Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# service-policy input aggflow1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>show mls qos aggregate-policer [aggregate-policer-name]</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show mls qos aggregate-policer transmit1</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy-running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Policing and Marking Overview
- Examples: Classifying, Policing, and Marking Traffic by Using Aggregate Policers, on page 463

**Configuring Egress Queue Characteristics**

Depending on the complexity of your network and your QoS solution, you might need to perform all of the tasks in the following modules. You need to make decisions about these characteristics:

- Which packets are mapped by DSCP or CoS value to each queue and threshold ID?
- What drop percentage thresholds apply to the queue-set (four egress queues per port), and how much reserved and maximum memory is needed for the traffic type?
• How much of the fixed buffer space is allocated to the queue-set?
• Does the bandwidth of the port need to be rate limited?
• How often should the egress queues be serviced and which technique (shaped, shared, or both) should be used?

**Related Topics**

- **Shaped or Shared Mode**, on page 423

**Configuration Guidelines**

Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:

- If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services this queue in shared mode.

**Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set**

You can guarantee the availability of buffers, set WTD thresholds, and configure the maximum allocation for a queue-set by using the `mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` global configuration command.

Each threshold value is a percentage of the queue’s allocated buffers, which you specify by using the `mls qos queue-set output qset-id buffers allocation1 ... allocation4` global configuration command. The queues use WTD to support distinct drop percentages for different traffic classes.

**Note**

The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to configure the memory allocation and to drop thresholds for a queue-set. This procedure is optional.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `queue-set qset-id`
4. `end`
5. `show mls qos interface [interface-id] buffers`
6. `copy running-config startup-config`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  configure terminal  
  Example:
  Switch# configure terminal | Enters global configuration mode. |
| **Step 2**
  interface interface-id  
  Example:
  Switch(config)# interface gigabitethernet1/0/1 | Specifies the port of the outbound traffic, and enter interface configuration mode. |
| **Step 3**
  queue-set qset-id  
  Example:
  Switch(config-id)# queue-set 2 | Maps the port to a queue-set.  
  For qset-id, enter the ID of the queue-set specified in Step 2. The range is 1 to 2. The default is 1. |
| **Step 4**
  end  
  Example:
  Switch(config-id)# end | Returns to privileged EXEC mode. |
| **Step 5**
  show mls qos interface [interface-id] buffers  
  Example:
  Switch# show mls qos interface buffers | Verifies your entries. |
| **Step 6**
  copy running-config startup-config  
  Example:
  Switch# copy-running-config startup-config | (Optional) Saves your entries in the configuration file.  
  To return to the default setting, use the no mls qos queue-set output qset-id buffers global configuration command. To return to the default WTD threshold percentages, use the no mls qos queue-set output qset-id threshold [queue-id] global configuration command. |

### Related Topics

- Queueing and Scheduling on Egress Queues
- Examples: Configuring Egress Queue Characteristics, on page 466

### Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID

You can prioritize traffic by placing packets with particular DSCPs or costs of service into certain queues and adjusting the queue thresholds so that packets with lower priorities are dropped.
The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to map DSCP or CoS values to an egress queue and to a threshold ID. This procedure is optional.

**SUMMARY STEPS**

1. configure terminal
2. Use one of the following:
   - `mls qos srr-queue output dscp-map queue queue-id threshold threshold-id dscp1...dscp8`
   - `mls qos srr-queue output cos-map queue queue-id threshold threshold-id cos1...cos8`
3. `mls qos srr-queue output cos-map queue queue-id threshold threshold-id cos1...cos8`
4. end
5. show mls qos maps
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Use one of the following:</td>
</tr>
</tbody>
</table>
| | • `mls qos srr-queue output dscp-map queue queue-id threshold threshold-id dscp1...dscp8`
| | • `mls qos srr-queue output cos-map queue queue-id threshold threshold-id cos1...cos8`
| Example: | Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11 |
| | Maps DSCP or CoS values to an egress queue and to a threshold ID. |
| | By default, DSCP values 0–15 are mapped to queue 2 and threshold 1. DSCP values 16–31 are mapped to queue 3 and threshold 1. DSCP values 32–39 and 48–63 are mapped to queue 4 and threshold 1. DSCP values 40–47 are mapped to queue 1 and threshold 1. |
| | By default, CoS values 0 and 1 are mapped to queue 2 and threshold 1. CoS values 2 and 3 are mapped to queue 3 and threshold 1. CoS values 4, 6, and 7 are mapped to queue 4 and threshold 1. CoS value 5 is mapped to queue 1 and threshold 1. |
| | • For `queue-id`, the range is 1 to 4. |
| | **Note** If you enabled 8 egress queues using the `mls qos srr-queue output queues 8` global configuration command, then the `queue-id` range would be from 1 to 8.
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For <code>threshold-id</code>, the range is 1 to 2. The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.</td>
</tr>
<tr>
<td>• For <code>dscp1...dscp8</code>, enter up to eight values, and separate each value with a space. The range is 0 to 63.</td>
</tr>
<tr>
<td>• For <code>cos1...cos8</code>, enter up to eight values, and separate each value with a space. The range is 0 to 7.</td>
</tr>
</tbody>
</table>

**Note**  
To return to the default DSCP output queue threshold map or the default CoS output queue threshold map, use the `no mls qos srr-queue output dscp-map` or the `no mls qos srr-queue output cos-map` global configuration command.

### Step 3

```bash
mls qos srr-queue output cos-map queue queue-id 
threshold threshold-id cos1...cos8
```

**Example:**

```
Switch(config)# mls qos srr-queue output cos-map queue 3 threshold 1 2 3
```

Maps CoS values to an egress queue and to a threshold ID. By default, CoS values 0 and 1 are mapped to queue 2 and threshold 1. CoS values 2 and 3 are mapped to queue 3 and threshold 1. CoS values 4, 6, and 7 are mapped to queue 4 and threshold 1. CoS value 5 is mapped to queue 1 and threshold 1.

- For `queue-id`, the range is 1 to 4.
- For `threshold-id`, the range is 1 to 2. The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.
- For `cos1...cos8`, enter up to eight values, and separate each value with a space. The range is 0 to 7.

**Note**  
To return to the default CoS output queue threshold map, use the `no mls qos srr-queue output cos-map` global configuration command.

### Step 4

```bash
end
```

**Example:**

```
Switch(config)# end
```

Returns to privileged EXEC mode.

### Step 5

```bash
show mls qos maps
```

**Example:**

```
Switch# show mls qos maps
```

Verifies your entries.

The DSCP output queue threshold map appears as a matrix. The d1 column specifies the most-significant digit of the DSCP number; the d2 row specifies the least-significant digit in the DSCP number. The intersection of the d1 and the d2 values provides the queue ID and threshold ID; for example, queue 2 and threshold 1 (02-01).
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The CoS output queue threshold map shows the CoS value in the top row and the corresponding queue ID and threshold ID in the second row; for example, queue 2 and threshold 2 (2-2).</td>
</tr>
</tbody>
</table>

**Step 6**

**copy running-config startup-config**

**Example:**

Switch# copy-running-config startup-config

(Optional) Saves your entries in the configuration file.

To return to the default DSCP output queue threshold map or the default CoS output queue threshold map, use the **no mls qos srr-queue output dscp-map** or the **no mls qos srr-queue output cos-map** global configuration command.

**Related Topics**

Queueing and Scheduling on Egress Queues
Examples: Configuring Egress Queue Characteristics, on page 466

**Configuring SRR Shaped Weights on Egress Queues**

You can specify how much of the available bandwidth is allocated to each queue. The ratio of the weights is the ratio of frequency in which the SRR scheduler sends packets from each queue.

You can configure the egress queues for shaped or shared weights, or both. Use shaping to smooth bursty traffic or to provide a smoother output over time.

Beginning in privileged EXEC mode, follow these steps to assign the shaped weights and to enable bandwidth shaping on the four egress queues mapped to a port. This procedure is optional.

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. srr-queue bandwidth shape weight1 weight2 weight3 weight4
4. end
5. show mls qos interface interface-id queueing
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| configure terminal
| Example:
| Switch# configure terminal

Enters global configuration mode.

| **Step 2**
| interface interface-id
| Example:
| Switch(config)# interface

Specifies the port of the outbound traffic, and enters interface configuration mode.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>gigabitethernet2/0/1</td>
<td></td>
</tr>
</tbody>
</table>

### Step 3

**srr-queue bandwidth shape** `weight1 weight2 weight3 weight4`

**Example:**

```
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

Assigns SRR weights to the egress queues. By default, `weight1` is set to 25; `weight2`, `weight3`, and `weight4` are set to 0, and these queues are in shared mode.

For `weight1 weight2 weight3 weight4`, enter the weights to control the percentage of the port that is shaped. The inverse ratio (1/weight) controls the shaping bandwidth for this queue. Separate each value with a space. The range is 0 to 65535.

If you configure a weight of 0, the corresponding queue operates in shared mode. The weight specified with the `srr-queue bandwidth shape` command is ignored, and the weights specified with the `srr-queue bandwidth share` interface configuration command for a queue come into effect. When configuring queues in the same queue-set for both shaping and sharing, make sure that you configure the lowest number queue for shaping.

The shaped mode overrides the shared mode.

To return to the default setting, use the `no srr-queue bandwidth shape` interface configuration command.

### Step 4

**end**

**Example:**

```
Switch(config-if)# end
```

Returns to privileged EXEC mode.

### Step 5

**show mls qos interface interface-id queueing**

**Example:**

```
Switch# show mls qos interface interface-id queueing
```

Verifies your entries.

### Step 6

**copy running-config startup-config**

**Example:**

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

To return to the default setting, use the `no srr-queue bandwidth shape` interface configuration command.

### Related Topics

- Queueing and Scheduling on Egress Queues
- Examples: Configuring Egress Queue Characteristics, on page 466
- SRR Shaping and Sharing
Configuring SRR Shared Weights on Egress Queues

In shared mode, the queues share the bandwidth among them according to the configured weights. The bandwidth is guaranteed at this level but not limited to it. For example, if a queue empties and does not require a share of the link, the remaining queues can expand into the unused bandwidth and share it among them.

With sharing, the ratio of the weights controls the frequency of dequeuing; the absolute values are meaningless.

**Note**
The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to assign the shared weights and to enable bandwidth sharing on the four egress queues mapped to a port. This procedure is optional.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `srr-queue bandwidth share weight1 weight2 weight3 weight4`
4. `end`
5. `show mls qos interface interface-id queueing`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch# configure terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specifies the port of the outbound traffic, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch(config)# interface gigabitethernet2/0/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>srr-queue bandwidth share weight1 weight2 weight3 weight4</code></td>
<td>Assigns SRR weights to the egress queues. By default, all four weights are 25 (1/4 of the bandwidth is allocated to each queue). For <code>weight1 weight2 weight3 weight4</code>, enter the weights to control the ratio of the frequency in which the SRR scheduler sends packets. Separate each value with a space. The range is 1 to 255. To return to the default setting, use the <code>no srr-queue bandwidth share</code> interface configuration command.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Switch(config-id)# srr-queue bandwidth share 1 2 3 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-id)# end</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>show mls qos interface interface-id queueing</code></td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show mls qos interface interface_id queueing</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy-running-config startup-config</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To return to the default setting, use the <code>no srr-queue bandwidth share</code> interface configuration command.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Queueing and Scheduling on Egress Queues
- Examples: Configuring Egress Queue Characteristics, on page 466
- SRR Shaping and Sharing

### Configuring the Egress Expedite Queue

You can ensure that certain packets have priority over all others by queuing them in the egress expedite queue. SRR services this queue until it is empty before servicing the other queues.

Beginning in privileged EXEC mode, follow these steps to enable the egress expedite queue. This procedure is optional.

### SUMMARY STEPS

1. `configure terminal`
2. `mls qos`
3. `interface interface-id`
4. `priority-queue out`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | **configure terminal** | Enters global configuration mode.  
Example:  
Switch# configure terminal |
| Step 2 | **mls qos** | Enables QoS on a switch.  
Example:  
Switch(config)# mls qos |
| Step 3 | **interface** *interface-id* | Specifies the egress port, and enters interface configuration mode.  
Example:  
Switch(config)# interface gigabitethernet1/0/1 |
| Step 4 | **priority-queue out** | Enables the egress expedite queue, which is disabled by default.  
When you configure this command, the SRR weight and queue size ratios are affected because there is one fewer queue participating in SRR. This means that *weight1* in the *srr-queue bandwidth shape* or the *srr-queue bandwidth share* command is ignored (not used in the ratio calculation).  
**Note** To disable the egress expedite queue, use the **no priority-queue out** interface configuration command.  
Example:  
Switch(config-if)# priority-queue out |
| Step 5 | **end** | Returns to privileged EXEC mode.  
Example:  
Switch(config-if)# end |
| Step 6 | **show running-config** | Verifies your entries.  
Example:  
Switch# show running-config |
| Step 7 | **copy running-config startup-config** | (Optional) Saves your entries in the configuration file.  
To disable the egress expedite queue, use the **no priority-queue out** interface configuration command.  
Example:  
<p>|</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**
- Queueing and Scheduling on Egress Queues
- Examples: Configuring Egress Queue Characteristics, on page 466

### Limiting the Bandwidth on an Egress Interface

You can limit the bandwidth on an egress port. For example, if a customer pays only for a small percentage of a high-speed link, you can limit the bandwidth to that amount.

**Note**
The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to limit the bandwidth on an egress port. This procedure is optional.

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. srr-queue bandwidth limit weight1
4. end
5. show mls qos interface [interface-id] queueing
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** configure terminal  
Example:  
Switch# configure terminal | Enters global configuration mode. |
| **Step 2** interface interface-id  
Example:  
Switch(config)# interface gigabitethernet2/0/1 | Specifies the port to be rate-limited, and enters interface configuration mode. |
### Purpose

**Command or Action**

**Step 3**

- `srr-queue bandwidth limit weight1`
  
  **Example:**
  ```
  Switch(config-if)# srr-queue bandwidth limit 80
  ```

  **Purpose:** Specifies the percentage of the port speed to which the port should be limited. The range is 10 to 90.

  **By default,** the port is not rate-limited and is set to 100 percent.

  **Note** To return to the default setting, use the `no srr-queue bandwidth limit` interface configuration command.

**Step 4**

- `end`
  
  **Example:**
  ```
  Switch(config-if)# end
  ```

  **Purpose:** Returns to privileged EXEC mode.

**Step 5**

- `show mls qos interface [interface-id] queueing`
  
  **Example:**
  ```
  Switch# show mls qos interface interface_id queueing
  ```

  **Purpose:** Verifies your entries.

**Step 6**

- `copy running-config startup-config`
  
  **Example:**
  ```
  Switch# copy-running-config startup-config
  ```

  **Purpose:** (Optional) Saves your entries in the configuration file.

  **Note** To return to the default setting, use the `no srr-queue bandwidth limit` interface configuration command.

### Related Topics

- Queueing and Scheduling on Egress Queues
- Examples: Configuring Egress Queue Characteristics, on page 466

### Monitoring Standard QoS

**Table 57: Commands for Monitoring Standard QoS on the Switch**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mls qos</code></td>
<td>Displays global QoS configuration information.</td>
</tr>
<tr>
<td>`show mls qos interface [interface-id] [queueing</td>
<td>statistics] show mls qos interface [interface-id] [</td>
</tr>
<tr>
<td>`show mls qos maps [cos-dscp</td>
<td>cos-output-q]`</td>
</tr>
<tr>
<td>`show running-config</td>
<td>include rewrite`</td>
</tr>
</tbody>
</table>
Configuration Examples for QoS

Example: Configuring Port to the DSCP- Trusted State and Modifying the DSCP-to-DSCP-Mutation Map

This example shows how to configure a port to the DSCP-trusted state and to modify the DSCP-to-DSCP-mutation map (named $gi1/0/2-mutation$) so that incoming DSCP values 10 to 13 are mapped to DSCP 30:

Switch(config)# mls qos map dscp-mutation gigabitethernet1/0/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gigabitethernet1/0/2-mutation
Switch(config-if)# end

Related Topics

  Configuring the DSCP Trust State on a Port Bordering Another QoS Domain

Examples: Classifying Traffic by Using ACLs

This example shows how to allow access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements is rejected.

Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
! (Note: all other access implicitly denied)

This example shows how to create an ACL that permits IP traffic from any source to any destination that has the DSCP value set to 32:

Switch(config)# access-list 100 permit ip any any dscp 32

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5

This example shows how to create an ACL that permits PIM traffic from any source to a destination group address of 224.0.0.2 with a DSCP set to 32:

Switch(config)# access-list 102 permit pim any 224.0.0.2 dscp 32
This example shows how to create an ACL that permits IPv6 traffic from any source to any destination that has the DSCP value set to 32:

```
Switch(config)# ipv6 access-list 100 permit ip any any dscp 32
```

This example shows how to create an ACL that permits IPv6 traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

```
Switch(config)# ipv6 access-list ipv6_Name_ACL permit ip host 10::1 host 10.1.1.2 precedence 5
```

This example shows how to create a Layer 2 MAC ACL with two permit statements. The first statement allows traffic from the host with MAC address 0001.0000.0001 to the host with MAC address 0002.0000.0001. The second statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 to the host with MAC address 0002.0000.0002.

```
Switch(config)# mac access-list extended maclist1
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
! (Note: all other access implicitly denied)
```

Related Topics

- Creating an IP Standard ACL for IPv4 Traffic, on page 428
- Creating an IP Extended ACL for IPv4 Traffic, on page 430
- Creating an IPv6 ACL for IPv6 Traffic, on page 431
- Creating a Layer 2 MAC ACL for Non-IP Traffic, on page 434

**Examples: Classifying Traffic by Using Class Maps**

This example shows how to configure the class map called `class1`. The `class1` has one match criterion, which is access list 103. It permits traffic from any host to any destination that matches a DSCP value of 10.

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# end
Switch#
```

This example shows how to create a class map called `class2`, which matches incoming traffic with DSCP values of 10, 11, and 12.

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

This example shows how to create a class map called `class3`, which matches incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map class3
```
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#

This example shows how to configure a class map to match IP DSCP and IPv6:

Switch(config)# Class-map cm-1
Switch(config-cmap)# match ip dscp 10
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# Class-map cm-2
Switch(config-cmap)# match ip dscp 20
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# Policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G1/0/1
Switch(config-if)# service-policy input pm1

This example shows how to configure a class map that applies to both IPv4 and IPv6 traffic:

Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
Switch(config)# Class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# Policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1

Related Topics
Classifying Traffic by Using Class Maps, on page 436
Classifying Traffic by Using Class Maps and Filtering IPv6 Traffic, on page 438
**Examples: Classifying, Policing, and Marking Traffic on Physical Ports Using Policy Maps**

This example shows how to create a policy map and attach it to an ingress port. In the configuration, the IP standard ACL permits traffic from network 10.1.0.0. For traffic matching this classification, the DSCP value in the incoming packet is trusted. If the matched traffic exceeds an average traffic rate of 48000 b/s and a normal burst size of 8000 bytes, its DSCP is marked down (based on the policed-DSCP map) and sent:

```plaintext
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map flow1t
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input flow1t
```

This example shows how to create a Layer 2 MAC ACL with two permit statements and attach it to an ingress port. The first permit statement allows traffic from the host with MAC address 0001.0000.0001 destined for the host with MAC address 0002.0000.0001. The second permit statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 destined for the host with MAC address 0002.0000.0002.

```plaintext
Switch(config)# mac access-list extended maclist1
Switch(config-ext-mac)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0 xns-idp
Switch(config-ext-mac)# exit
Switch(config)# mac access-list extended maclist2
Switch(config-ext-mac)# permit 0001.0000.0003 0.0.0 0002.0000.0003 0.0.0
Switch(config-ext-mac)# permit 0001.0000.0004 0.0.0 0002.0000.0004 0.0.0 aarp
Switch(config-ext-mac)# exit
Switch(config)# class-map macclass1
Switch(config-cmap)# match access-group maclist1
Switch(config-cmap)# exit
Switch(config)# policy-map macpolicy1
Switch(config-pmap)# class macclass1
Switch(config-pmap-c)# set dscp 63
Switch(config-pmap-c)# exit
Switch(config)# policy-map macpolicy2
Switch(config-pmap-c)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input macpolicy1
```

This example shows how to create a class map that applies to both IPv4 and IPv6 traffic with the default class applied to unclassified traffic:

```plaintext
Switch(config)# ip access-list 101 permit ip any any
Switch(config)# ipv6 access-list ipv6-any permit ip any any
```
Switch(config)# class-map cm-1
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# exit
Switch(config)# class-map cm-2
Switch(config-cmap)# match access-group name ipv6-any
Switch(config-cmap)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1

Related Topics
Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps, on page 440
Policy Map on Physical Port

Examples: Classifying, Policing, and Marking Traffic by Using Aggregate Policers

This example shows how to create an aggregate policer and attach it to multiple classes within a policy map. In the configuration, the IP ACLs permit traffic from network 10.1.0.0 and from host 11.3.1.1. For traffic coming from network 10.1.0.0, the DSCP in the incoming packets is trusted. For traffic coming from host 11.3.1.1, the DSCP in the packet is changed to 56. The traffic rate from the 10.1.0.0 network and from host 11.3.1.1 is policed. If the traffic exceeds an average rate of 48000 b/s and a normal burst size of 8000 bytes, its DSCP is marked down (based on the policed-DSCP map) and sent. The policy map is attached to an ingress port.

Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap-c)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap-c)# class class-default

QoS
Examples: Configuring DSCP Maps

This example shows how to modify and display the CoS-to-DSCP map:

```plaintext
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps cos-dscp
```

Cos-dscp map:

```
cos: 0 1 2 3 4 5 6 7
--------------------------------
dscp: 10 15 20 25 30 35 40 45
```

This example shows how to modify and display the IP-precedence-to-DSCP map:

```plaintext
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp
```

IpPrecedence-dscp map:

```
ipprec: 0 1 2 3 4 5 6 7
--------------------------------
dscp: 10 15 20 25 30 35 40 45
```

This example shows how to map DSCP 50 to 57 to a marked-down DSCP value of 0:

```plaintext
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp
```

Policed-dscp map:

```
d1 : d2 0 1 2 3 4 5 6 7 8 9
---------------------------------------
 0 : 00 01 02 03 04 05 06 07 08 09
 1 : 10 11 12 13 14 15 16 17 18 19
 2 : 20 21 22 23 24 25 26 27 28 29
 3 : 30 31 32 33 34 35 36 37 38 39
 4 : 40 41 42 43 44 45 46 47 48 49
 5 : 00 00 00 00 00 00 00 00 58 59
 6 : 60 61 62 63
```
This policed-DSCP map, the marked-down DSCP values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the marked-down value. For example, an original DSCP value of 53 corresponds to a marked-down DSCP value of 0.

This example shows how to map DSCP values 0, 8, 16, 24, 32, 40, 48, and 50 to CoS value 0 and to display the map:

```
Switch(config)# ml qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
  d1  : d2 0 1 2 3 4 5 6 7 8 9
  ---------------------------
  0 : 00 00 00 00 00 00 00 00 00 1
  1 : 01 01 01 01 01 01 00 02 02 02
  2 : 02 02 02 02 00 03 03 03 03 03
  3 : 03 03 00 04 04 04 04 04 04 04
  4 : 00 05 05 05 05 05 05 05 05 05
  5 : 00 06 06 06 06 06 06 07 07 07
  6 : 07 07 07 07
```

In the above DSCP-to-CoS map, the CoS values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the DSCP; the d2 row specifies the least-significant digit of the DSCP. The intersection of the d1 and d2 values provides the CoS value. For example, in the DSCP-to-CoS map, a DSCP value of 08 corresponds to a CoS value of 0.

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remains as specified in the null map):

```
Switch(config)# ml qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# ml qos map dscp-mutation mutation1 8 9 to 10
Switch(config)# ml qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# ml qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ml qos trust dscp
Switch(config-if)# ml qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
  mutation1:
    d1 : d2 0 1 2 3 4 5 6 7 8 9
    ---------------------------
    0 : 00 00 00 00 00 00 00 00 10 10
    1 : 10 10 10 10 14 15 16 17 18 19
    2 : 20 20 20 23 24 25 26 27 28 29
    3 : 30 30 30 30 35 36 37 38 39
    4 : 40 41 42 43 44 45 46 47 48 49
    5 : 50 51 52 53 54 55 56 57 58 59
    6 : 60 61 62 63
```

Note
In this policed-DSCP map, the marked-down DSCP values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the marked-down value. For example, an original DSCP value of 53 corresponds to a marked-down DSCP value of 0.

This example shows how to map DSCP values 0, 8, 16, 24, 32, 40, 48, and 50 to CoS value 0 and to display the map:

```
Switch(config)# ml qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
  d1  : d2 0 1 2 3 4 5 6 7 8 9
  ---------------------------
  0 : 00 00 00 00 00 00 00 00 00 1
  1 : 01 01 01 01 01 01 00 02 02 02
  2 : 02 02 02 02 00 03 03 03 03 03
  3 : 03 03 00 04 04 04 04 04 04 04
  4 : 00 05 05 05 05 05 05 05 05 05
  5 : 00 06 06 06 06 06 06 07 07 07
  6 : 07 07 07 07
```

Note
In the above DSCP-to-CoS map, the CoS values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the DSCP; the d2 row specifies the least-significant digit of the DSCP. The intersection of the d1 and d2 values provides the CoS value. For example, in the DSCP-to-CoS map, a DSCP value of 08 corresponds to a CoS value of 0.

This example shows how to define the DSCP-to-DSCP-mutation map. All the entries that are not explicitly configured are not modified (remains as specified in the null map):

```
Switch(config)# ml qos map dscp-mutation mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# ml qos map dscp-mutation mutation1 8 9 to 10
Switch(config)# ml qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# ml qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ml qos trust dscp
Switch(config-if)# ml qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
  mutation1:
    d1  : d2 0 1 2 3 4 5 6 7 8 9
    ---------------------------
    0 : 00 00 00 00 00 00 00 00 10 10
    1 : 10 10 10 10 14 15 16 17 18 19
    2 : 20 20 20 23 24 25 26 27 28 29
    3 : 30 30 30 30 35 36 37 38 39
    4 : 40 41 42 43 44 45 46 47 48 49
    5 : 50 51 52 53 54 55 56 57 58 59
    6 : 60 61 62 63
```
In the above DSCP-to-DSCP-mutation map, the mutated values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the mutated value. For example, a DSCP value of 12 corresponds to a mutated value of 10.

### Related Topics
- Configuring the CoS-to-DSCP Map
- Configuring the IP-Precedence-to-DSCP Map
- Configuring the Policed-DSCP Map
- Configuring the DSCP-to-CoS Map
- Configuring the DSCP-to-DSCP-Mutation Map

### Examples: Configuring Egress Queue Characteristics

This example shows how to configure bandwidth shaping on queue 1. Because the weight ratios for queues 2, 3, and 4 are set to 0, these queues operate in shared mode. The bandwidth weight for queue 1 is 1/8, which is 12.5 percent:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```

This example shows how to configure the weight ratio of the SRR scheduler running on an egress port. Four queues are used, and the bandwidth ratio allocated for each queue in shared mode is 1/(1+2+3+4), 2/(1+2+3+4), 3/(1+2+3+4), and 4/(1+2+3+4), which is 10 percent, 20 percent, 30 percent, and 40 percent for queues 1, 2, 3, and 4. This means that queue 4 has four times the bandwidth of queue 1, twice the bandwidth of queue 2, and one-and-a-third times the bandwidth of queue 3.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
```

This example shows how to enable the egress expedite queue when the SRR weights are configured. The egress expedite queue overrides the configured SRR weights.

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# srr-queue bandwidth shape 25 0 0 0
Switch(config-if)# srr-queue bandwidth share 30 20 25 25
Switch(config-if)# priority-queue out
Switch(config-if)# end
```

This example shows how to limit the bandwidth on a port to 80 percent:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# srr-queue bandwidth limit 80
```

When you configure this command to 80 percent, the port is idle 20 percent of the time. The line rate drops to 80 percent of the connected speed, which is 800 Mb/s. These values are not exact because the hardware adjusts the line rate in increments of six.
Related Topics

- Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set, on page 448
- Queueing and Scheduling on Egress Queues
- Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID, on page 449
- Configuring SRR Shaped Weights on Egress Queues, on page 452
- Configuring SRR Shared Weights on Egress Queues, on page 454
- Configuring the Egress Expedite Queue, on page 455
- Limiting the Bandwidth on an Egress Interface, on page 457

Where to Go Next

Review the auto-QoS documentation to see if you can use these automated capabilities for your QoS configuration.
PART IX

Security

• Security Features Overview, on page 471
• Preventing Unauthorized Access, on page 475
• Controlling Switch Access with Passwords and Privilege Levels, on page 477
• Configuring TACACS+, on page 495
• Configuring RADIUS, on page 539
• Configuring Accounting, on page 581
• Configuring Local Authentication and Authorization, on page 611
• MAC Authentication Bypass, on page 615
• Password Strength and Management for Common Criteria, on page 627
• AAA-SERVER-MIB Set Operation, on page 637
• Configuring Secure Shell, on page 645
• Secure Shell Version 2 Support, on page 665
• X.509v3 Certificates for SSH Authentication, on page 693
• Configuring Secure Socket Layer HTTP, on page 703
• Certification Authority Interoperability, on page 717
• Access Control List Overview, on page 735
• Configuring IPv4 Access Control Lists, on page 745
• IPv6 Access Control Lists, on page 783
• Configuring DHCP, on page 799
• Configuring IEEE 802.1x Port-Based Authentication, on page 823
• Configuring Port-Based Traffic Control, on page 863
Security Features Overview

The switch supports a LAN base image or a LAN lite image with a reduced feature set, depending on switch hardware. The security features are as follows:

- **Web Authentication**— Allows a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser.
- **Local Web Authentication Banner**— A custom banner or an image file displayed at a web authentication login screen.
- **IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute**
- **Password-protected access (read-only and read-write access) to management interfaces (device manager, Network Assistant, and the CLI) for protection against unauthorized configuration changes**
- **Multilevel security for a choice of security level, notification, and resulting actions**
- **Static MAC addressing for ensuring security**
- **Protected port option for restricting the forwarding of traffic to designated ports on the same switch**
- **Port security option for limiting and identifying MAC addresses of the stations allowed to access the port**
- **VLAN aware port security option to shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port.**
- **Port security aging to set the aging time for secure addresses on a port.**
- **Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate.**
- **BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs.**
- **Standard and extended IP access control lists (ACLs) for defining inbound security policies on Layer 2 interfaces (port ACLs).**
- **Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces.**
• Source and destination MAC-based ACLs for filtering non-IP traffic.

• DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers.

• IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings.

• Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.

  This feature is not supported on LanLite images on Catalyst 2960-X Series Switches.

• IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These 802.1x features are supported:
  • Support for single-host, multi-host, multi-auth, and multi-domain-auth modes.
  • Multidomain authentication (MDA) to allow both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to independently authenticate on the same IEEE 802.1x-enabled switch port.
  • Dynamic voice virtual LAN (VLAN) for MDA to allow a dynamic voice VLAN on an MDA-enabled port.
  • VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN.
  • Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.
  • Port security for controlling access to 802.1x ports.
  • Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port.
  • IP phone detection enhancement to detect and recognize a Cisco IP phone.
  • Guest VLAN to provide limited services to non-802.1x-compliant users.
  • Restricted VLAN to provide limited services to users who are 802.1x compliant, but do not have the credentials to authenticate via the standard 802.1x processes.
  • 802.1x accounting to track network usage.
  • 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch.
  • Voice aware 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs.
  • MAC authentication bypass (MAB) to authorize clients based on the client MAC address.
  • Network Admission Control (NAC) Layer 2 802.1x validation of the antivirus condition or posture of endpoint systems or clients before granting the devices network access.

  **Note**  
  NAC is not supported on LanLite images.
- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.

Note NEAT is not supported on LanLite images.

- IEEE 802.1x with open access to allow a host to access the network before being authenticated.

Note This feature is not supported on LanLite images.

- IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch.

- Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs.

Note This feature is not supported on LanLite images.

- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.

- Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port.

- TACACS+, a proprietary feature for managing network security through a TACACS server for both IPv4 and IPv6.

- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services for both IPv4 and IPv6.

- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.

- Secure Socket Layer (SSL) Version 3.0 support for the HTTP 1.1 server authentication, encryption, and message integrity and HTTP client authentication to allow secure HTTP communications (requires the cryptographic version of the software).

- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute.

- Support for IP source guard on static hosts.

- RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Identity Services Engine, or Cisco Secure ACS to reinitialize authentication, and apply to the new policies.

- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
This feature is not supported on LanLite images.

- Support for critical VLAN—multi-host/multi-auth enabled ports are placed in a critical VLAN in order to permit access to critical resources if AAA server becomes unreachable.

This feature is not supported on LanLite images.

- Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.

- VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.

- MAC move to allow hosts (including the hosts connected behind an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.

- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.

- Support for Cisco TrustSec SXP protocol. This feature is not supported on LanLite images.
Preventing Unauthorized Access

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Preventing Unauthorized Access

You can prevent unauthorized users from reconfiguring your switch and viewing configuration information. Typically, you want network administrators to have access to your switch while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your switch, you should configure one or more of these security features:

- At a minimum, you should configure passwords and privileges at each switch port. These passwords are locally stored on the switch. When users attempt to access the switch through a port or line, they must enter the password specified for the port or line before they can access the switch.

- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

- If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information.
You can also enable the login enhancements feature, which logs both failed and unsuccessful login attempts. Login enhancements can also be configured to block future login attempts after a set number of unsuccessful attempts are made. For more information, see the Cisco IOS Login Enhancements documentation.

Related Topics

- Configuring Username and Password Pairs, on page 486
- TACACS+ and Switch Access, on page 497
- Setting a Telnet Password for a Terminal Line, on page 485
Controlling Switch Access with Passwords and Privilege Levels

• Finding Feature Information, on page 477
• Restrictions for Controlling Switch Access with Passwords and Privileges, on page 477
• Information About Passwords and Privilege Levels, on page 478
• How to Control Switch Access with Passwords and Privilege Levels, on page 480
• Monitoring Switch Access, on page 492
• Configuration Examples for Setting Passwords and Privilege Levels, on page 492
• Additional References, on page 493

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Controlling Switch Access with Passwords and Privileges

The following are the restrictions for controlling switch access with passwords and privileges:

• Disabling password recovery will not work if you have set the switch to boot up manually by using the boot manual global configuration command. This command produces the boot loader prompt (switch:) after the switch is power cycled.

Related Topics

Disabling Password Recovery, on page 483
Password Recovery, on page 478
Information About Passwords and Privilege Levels

Default Password and Privilege Level Configuration

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

This table shows the default password and privilege level configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file.</td>
</tr>
<tr>
<td>Enable secret password and privilege level</td>
<td>No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.</td>
</tr>
<tr>
<td>Line password</td>
<td>No password is defined.</td>
</tr>
</tbody>
</table>

Additional Password Security

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the `enable password` or `enable secret` global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

We recommend that you use the `enable secret` command because it uses an improved encryption algorithm. If you configure the `enable secret` command, it takes precedence over the `enable password` command; the two commands cannot be in effect simultaneously.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

Related Topics
- Protecting Enable and Enable Secret Passwords with Encryption, on page 482
- Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 492

Password Recovery

By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set
the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted.

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

To re-enable password recovery, use the `service password-recovery` global configuration command.

**Related Topics**
- Disabling Password Recovery, on page 483
- Restrictions for Controlling Switch Access with Passwords and Privileges, on page 477

**Terminal Line Telnet Configuration**

When you power-up your switch for the first time, an automatic setup program runs to assign IP information and to create a default configuration for continued use. The setup program also prompts you to configure your switch for Telnet access through a password. If you did not configure this password during the setup program, you can configure it when you set a Telnet password for a terminal line.

**Related Topics**
- Setting a Telnet Password for a Terminal Line, on page 485
- Example: Setting a Telnet Password for a Terminal Line, on page 492

**Username and Password Pairs**

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

**Related Topics**
- Configuring Username and Password Pairs, on page 486

**Privilege Levels**

Cisco switches (and other devices) use privilege levels to provide password security for different levels of switch operation. By default, the Cisco IOS software operates in two modes (privilege levels) of password security: user EXEC (Level 1) and privileged EXEC (Level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

**Privilege Levels on Lines**

Users can override the privilege level you set using the `privilege level` line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the `disable` command. If users know the password to a higher privilege level, they can use that password to enable the
higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

For example, if you want many users to have access to the clear line command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the configure command, you can assign it level 3 security and distribute that password to a more restricted group of users.

Command Privilege Levels

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the show ip traffic command to level 15, the show commands and show ip commands are automatically set to privilege level 15 unless you set them individually to different levels.

Related Topics

- Setting the Privilege Level for a Command, on page 488
- Example: Setting the Privilege Level for a Command, on page 493
- Changing the Default Privilege Level for Lines, on page 490
- Logging into and Exiting a Privilege Level, on page 491

How to Control Switch Access with Passwords and Privilege Levels

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Follow these steps to set or change a static enable password:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. enable password \textit{password}
4. end
5. show running-config
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>\textbullet{} Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>enable password password</code></td>
<td>Defines a new password or changes an existing password for access to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# enable password secret321</code></td>
<td>By default, no password is defined.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

Example: Setting or Changing a Static Enable Password, on page 492
Protecting Enable and Enable Secret Passwords with Encryption

Follow these steps to establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. Use one of the following:
   - `enable password [level level] {password encryption-type encrypted-password}`
   - `enable secret [level level] {password encryption-type encrypted-password}`
4. service password-encryption
5. end
6. show running-config
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

**Example:**

```
Switch> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

| **Step 2**

**Example:**

```
Switch# configure terminal
```

Enters global configuration mode.

| **Step 3**

**Example:**

```
Switch(config)# enable password example102
```

or

```
Switch(config)# enable secret level 1 password secret123sample
```

- Defines a new password or changes an existing password for access to privileged EXEC mode.
- Defines a secret password, which is saved using a nonreversible encryption method.
  - (Optional) For `level`, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).
  - For `password`, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>* (Optional) For <em>encryption-type</em>, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>If you specify an encryption type and then enter a clear text password, you cannot re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.</td>
</tr>
</tbody>
</table>
| **Step 4** service password-encryption  
Example:  
Switch(config)# service password-encryption | (Optional) Encrypts the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file. |
| **Step 5** end  
Example:  
Switch(config)# end | Returns to privileged EXEC mode. |
| **Step 6** show running-config  
Example:  
Switch# show running-config | Verifies your entries. |
| **Step 7** copy running-config startup-config  
Example:  
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

### Related Topics
- Additional Password Security, on page 478
- Example: Protecting Enable and Enable Secret Passwords with Encryption, on page 492

### Disabling Password Recovery

Follow these steps to disable password recovery to protect the security of your switch:
Before you begin

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

SUMMARY STEPS

1. enable
2. configure terminal
3. system disable password recovery switch <1-9>
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        | Enters global configuration mode. |
| `configure terminal` | |
| **Example:**      |         |
| `Switch# configure terminal` | |

| **Step 3**        | Disables password recovery. |
| `system disable password recovery switch <1-9>` | • `all` - Sets the configuration on switches in stack. |
| `Example:`        | • `<1-9>` - Sets the configuration on the Switch Number selected. |
| `Switch(config)# system disable password recovery switch all` | This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but it is not part of the file system and is not accessible by any user. |

| **Step 4**        | Returns to privileged EXEC mode. |
| `end`             | |
| `Example:`        |         |
| `Switch(config)# end` | |
What to do next

To remove disable password recovery, use the no system disable password recovery switch all global configuration command.

Related Topics

Password Recovery, on page 478
Restrictions for Controlling Switch Access with Passwords and Privileges, on page 477

Setting a Telnet Password for a Terminal Line

Beginning in user EXEC mode, follow these steps to set a Telnet password for the connected terminal line:

Before you begin

- Attach a PC or workstation with emulation software to the switch console port, or attach a PC to the Ethernet management port.
- The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.

SUMMARY STEPS

1. enable
2. configure terminal
3. line vty 0 15
4. password password
5. end
6. show running-config
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable&lt;br&gt;Example: Switch&gt; enable</td>
<td>Note: If a password is required for access to privileged EXEC mode, you will be prompted for it. Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal&lt;br&gt;Example: Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>line vty 0 15&lt;br&gt;Example:</td>
<td>Configures the number of Telnet sessions (lines), and enters line configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring Username and Password Pairs

Follow these steps to configure username and password pairs:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `username name [privilege level] {password encryption-type password}`
4. Use one of the following:
   - `line console 0`
   - `line vty 0 15`
5. `login local`

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# line vty 0 15</code></td>
<td>There are 16 possible sessions on a command-capable Switch. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.</td>
</tr>
</tbody>
</table>

**Step 4**

`password password`

**Example:**

`Switch(config-line)# password abcxyz543`

Sets a Telnet password for the line or lines.

For `password`, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.

**Step 5**

`end`

**Example:**

`Switch(config-line)# end`

Returns to privileged EXEC mode.

**Step 6**

`show running-config`

**Example:**

`Switch# show running-config`

Verifies your entries.

**Step 7**

`copy running-config startup-config`

**Example:**

`Switch# copy running-config startup-config`

(Optional) Saves your entries in the configuration file.

---

**Related Topics**

- [Preventing Unauthorized Access](#)
- [Terminal Line Telnet Configuration](#)
- Example: Setting a Telnet Password for a Terminal Line

---

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
6. **end**  
7. **show running-config**  
8. **copy running-config startup-config**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| Example: Switch> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Switch# configure terminal | |
| **Step 3** username name [privilege level] [password encryption-type password] | Sets the username, privilege level, and password for each user.  
• For name, specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed.  
• You can configure a maximum of 12000 clients each, for both username and MAC filter.  
• (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access.  
• For encryption-type, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow.  
• For password, specify the password the user must enter to gain access to the Switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command. |
| Example:  
Switch(config)# username adamsample privilege 1 password secret456  
Switch(config)# username 111111111111 mac attribute | |
| **Step 4** Use one of the following:  
• line console 0  
• line vty 0 15 | Enters line configuration mode, and configures the console port (line 0) or the VTY lines (line 0 to 15). |
| Example:  
Switch(config)# line console 0  
or  
Switch(config)# line vty 15 | |
## Setting the Privilege Level for a Command

Follow these steps to set the privilege level for a command:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `privilege mode level level command`
4. `enable password level level password`
5. `end`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td><em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

### Step 2

**configure terminal**  
**Example:**

Switch# configure terminal

**Purpose:** Enters global configuration mode.

### Step 3

**privilege mode level level command**  
**Example:**

Switch(config)# privilege exec level 14 configure

**Purpose:** Sets the privilege level for a command.  
- For `mode`, enter `configure` for global configuration mode, `exec` for EXEC mode, `interface` for interface configuration mode, or `line` for line configuration mode.
- For `level`, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the `enable` password.
- For `command`, specify the command to which you want to restrict access.

### Step 4

**enable password level level password**  
**Example:**

Switch(config)# enable password level 14 SecretPswd14

**Purpose:** Specifies the password to enable the privilege level.  
- For `level`, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.
- For `password`, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.

### Step 5

**end**  
**Example:**

Switch(config)# end

**Purpose:** Returns to privileged EXEC mode.

### Step 6

**copy running-config startup-config**  
**Example:**

Switch# copy running-config startup-config

**Purpose:** (Optional) Saves your entries in the configuration file.

### Related Topics

- Privilege Levels, on page 479  
- Example: Setting the Privilege Level for a Command, on page 493
Changing the Default Privilege Level for Lines

Follow these steps to change the default privilege level for the specified line:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `line vty line`
4. `privilege level level`
5. `end`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
Example:  
`Switch> enable`
| | | • Enter your password if prompted. |
| Step 2 | `configure terminal` | Enters global configuration mode.  
Example:  
`Switch(config)# configure terminal` |
| Step 3 | `line vty line` | Selects the virtual terminal line on which to restrict access.  
Example:  
`Switch(config)# line vty 10` |
| Step 4 | `privilege level level` | Changes the default privilege level for the line.  
For `level`, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the `enable` password.  
Example:  
`Switch(config)# privilege level 15` |
| Step 5 | `end` | Returns to privileged EXEC mode.  
Example:  
`Switch(config)# end` |
| Step 6 | `copy running-config startup-config` | (Optional) Saves your entries in the configuration file.  
Example: |

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
**What to do next**

Users can override the privilege level you set using the `privilege level` line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the `disable` command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

**Related Topics**

- Privilege Levels, on page 479

---

### Logging into and Exiting a Privilege Level

Beginning in user EXEC mode, follow these steps to log into a specified privilege level and exit a specified privilege level.

**SUMMARY STEPS**

1. `enable level`
2. `disable level`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable level</code></td>
<td>Logs in to a specified privilege level. Following the example, Level 15 is privileged EXEC mode. For level, the range is 0 to 15.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable 15</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>disable level</code></td>
<td>Exits to a specified privilege level. Following the example, Level 1 is user EXEC mode. For level, the range is 0 to 15.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# disable 1</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Privilege Levels, on page 479
Monitoring Switch Access

Table 59: Commands for Displaying DHCP Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show privilege</td>
<td>Displays the privilege level configuration.</td>
</tr>
</tbody>
</table>

Configuration Examples for Setting Passwords and Privilege Levels

Example: Setting or Changing a Static Enable Password

This example shows how to change the enable password to l1u2c3k4y5. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Switch(config)# enable password l1u2c3k4y5
```

Related Topics

- Setting or Changing a Static Enable Password, on page 480

Example: Protecting Enable and Enable Secret Passwords with Encryption

This example shows how to configure the encrypted password $1$FaD0$Xyti5Rkl3LoyxzS8 for privilege level 2:

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkl3LoyxzS8
```

Related Topics

- Protecting Enable and Enable Secret Passwords with Encryption, on page 482
- Additional Password Security, on page 478

Example: Setting a Telnet Password for a Terminal Line

This example shows how to set the Telnet password to let45me67in89:

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

Related Topics

- Setting a Telnet Password for a Terminal Line, on page 485
- Terminal Line Telnet Configuration, on page 479
Example: Setting the Privilege Level for a Command

This example shows how to set the `configure` command to privilege level 14 and define `SecretPswd14` as the password users must enter to use level 14 commands:

Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14

Related Topics
- Setting the Privilege Level for a Command, on page 488
- Privilege Levels, on page 479

Additional References

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Configuring TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization and accounting (AAA) and can be enabled only through AAA commands.

- Finding Feature Information, on page 495
- Prerequisites for TACACS+, on page 495
- Restrictions for TACACS+, on page 496
- Information About TACACS+, on page 497
- How to Configure TACACS+, on page 521
- Configuration Examples for TACACS+, on page 532
- Additional References for TACACS+, on page 536
- Feature Information for TACACS+, on page 537

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for TACACS+

The following are the prerequisites for set up and configuration of switch access with TACACS+ (must be performed in the order presented):

1. Configure the switches with the TACACS+ server addresses.
2. Set an authentication key.
3. Configure the key from Step 2 on the TACACS+ servers.
4. Enable authentication, authorization, and accounting (AAA).
5. Create a login authentication method list.
6. Apply the list to the terminal lines.
7. Create an authorization and accounting method list.

The following are the prerequisites for controlling switch access with TACACS+:

- You must have access to a configured TACACS+ server to configure TACACS+ features on your switch. Also, you must have access to TACACS+ services maintained in a database on a TACACS+ daemon typically running on a LINUX or Windows workstation.
- We recommend a redundant connection between a switch stack and the TACACS+ server. This is to help ensure that the TACACS+ server remains accessible in case one of the connected stack members is removed from the switch stack.
- You need a system running the TACACS+ daemon software to use TACACS+ on your switch.
- To use TACACS+, it must be enabled.
- Authorization must be enabled on the switch to be used.
- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- To use any of the AAA commands listed in this section or elsewhere, you must first enable AAA with the `aaa new-model` command.
- At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting.
- The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named `default`). The default method list is automatically applied to all ports except those that have a named method list explicitly defined. A defined method list overrides the default method list.
- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

**Restrictions for TACACS+**

TACACS+ can be enabled only through AAA commands.
Information About TACACS+

TACACS+ and Switch Access

This section describes TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over the authentication and authorization processes. It is facilitated through authentication, authorization, accounting (AAA) and can be enabled only through AAA commands.

Related Topics
Preventing Unauthorized Access, on page 475

TACACS+ Overview

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—individually. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The goal of TACACS+ is to provide a method for managing multiple network access points from a single management service. Your switch can be a network access server along with other Cisco routers and access servers.

Figure 43: Typical TACACS+ Network Configuration

TACACS+, administered through the AAA security services, can provide these services:

- Authentication—Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.
The authentication facility can conduct a dialog with the user (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother’s maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to user screens. For example, a message could notify users that their passwords must be changed because of the company’s password aging policy.

- **Authorization**—Provides fine-grained control over user capabilities for the duration of the user’s session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on what commands a user can execute with the TACACS+ authorization feature.

- **Accounting**—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track user activity for a security auditor to provide information for user billing. Accounting records include user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the switch and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the switch and the TACACS+ daemon are encrypted.

### TACACS+ Operation

When a user attempts a simple ASCII login by authenticating to a switch using TACACS+, this process occurs:

1. When the connection is established, the switch contacts the TACACS+ daemon to obtain a username prompt to show to the user. The user enters a username, and the switch then contacts the TACACS+ daemon to obtain a password prompt. The switch displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.

   TACACS+ allows a dialog between the daemon and the user until the daemon receives enough information to authenticate the user. The daemon prompts for a username and password combination, but can include other items, such as the user’s mother’s maiden name.

2. The switch eventually receives one of these responses from the TACACS+ daemon:
   
   - **ACCEPT**—The user is authenticated and service can begin. If the switch is configured to require authorization, authorization begins at this time.
   
   - **REJECT**—The user is not authenticated. The user can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
   
   - **ERROR**—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the switch. If an ERROR response is received, the switch typically tries to use an alternative method for authenticating the user.
   
   - **CONTINUE**—The user is prompted for additional authentication information.

   After authentication, the user undergoes an additional authorization phase if authorization has been enabled on the switch. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that user and the services that the user can access:
Method List

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

TACACS AV Pairs

The network access server implements TACACS+ authorization and accounting functions by transmitting and receiving TACACS+ attribute-value (AV) pairs for each user session.

TACACS Authentication and Authorization AV Pairs

The following table lists and describes the supported TACACS+ authentication and authorization AV pairs and specifies the Cisco IOS release in which they are implemented.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>11.0</th>
<th>11.1</th>
<th>11.2</th>
<th>11.3</th>
<th>12.0</th>
<th>12.1</th>
<th>12.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>acl=x</td>
<td>ASCII number representing a connection access list. Used only when service=shell.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>addr=x</td>
<td>A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=10.2.3.4.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>addr-pool=x</td>
<td>Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>Note that addr-pool works in conjunction with local pooling. It specifies the name of a local pool (which must be preconfigured on the network access server). Use the ip-local pool command to declare local pools. For example:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip address-pool local</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip local pool boo 10.0.0.1 10.0.0.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip local pool moo 10.0.0.1 10.0.0.20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can then use TACACS+ to return addr-pool=boo or addr-pool=moo to indicate the address pool from which you want to get this remote node’s address.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>autocmd=x</td>
<td>Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet example.com). Used only with service=shell.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>callback-dialstring</td>
<td>Sets the telephone number for a callback (for example: callback-dialstring=408-555-1212). Value is NULL, or a dial-string. A NULL value indicates that the service might choose to get the dial string through other means. Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>callback-line</td>
<td>The number of a TTY line to use for callback (for example: callback-line=4). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>callback-rotary</td>
<td>The number of a rotary group (between 0 and 100 inclusive) to use for callback (for example: callback-rotary=34). Used with service=arap, service=slip, service=ppp, service=shell. Not valid for ISDN.</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>cmd-arg=x</td>
<td>An argument to a shell (EXEC) command. This indicates an argument for the shell command that is to be run. Multiple cmd-arg attributes can be specified, and they are order dependent.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>cmd=x</td>
<td>A shell (EXEC) command. This indicates the command name for a shell command that is to be run. This attribute must be specified if service equals “shell.” A NULL value indicates that the shell itself is being referred to.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>data-service</td>
<td>Used with the service=outbound and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>dial-number</td>
<td>Defines the number to dial. Used with the service=outbound and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>dns-servers=</td>
<td>Identifies a DNS server (primary or secondary) that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each DNS server is entered in dotted decimal format.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>force-56</td>
<td>Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available. To turn on this attribute, use the “true” value (force-56=true). Any other value is treated as false. Used with the service=outbound and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>gw-password</td>
<td>Specifies the password for the home gateway during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>idletime=x</td>
<td>Sets a value, in minutes, after which an idle session is terminated. A value of zero indicates no timeout.</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>inacl#&lt;n&gt;</td>
<td>ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Used with service=ppp and protocol=ip, and service service=ppp and protocol =ipx. Per-user access lists do not currently work with ISDN interfaces.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>inacl=x</td>
<td>ASCII identifier for an interface input access list. Used with service=ppp and protocol=ip. Per-user access lists do not currently work with ISDN interfaces.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>interface-config#&lt;n&gt;</td>
<td>Specifies user-specific AAA interface configuration information with Virtual Profiles. The information that follows the equal sign (=) can be any Cisco IOS interface configuration command. Multiple instances of the attributes are allowed, but each instance must have a unique number. Used with service=ppp and protocol=lcp. <strong>Note</strong> This attribute replaces the “interface-config=” attribute.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>ip-addresses</td>
<td>Space-separated list of possible IP addresses that can be used for the end-point of a tunnel. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-busy-disconnect</td>
<td>If a vpdn-group on an LNS uses a virtual-template that is configured to be pre-cloned, this attribute will control the disposition of a new L2TP session that finds no pre-cloned interface to which to connect. If the attribute is true (the default), the session will be disconnected by the LNS. Otherwise, a new interface will be cloned from the virtual-template. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-cm-local-window-size</td>
<td>Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-drop-out-of-order</td>
<td>Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-hello-interval</td>
<td>Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-hidden-avp</td>
<td>When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>l2tp-nosession-timeout</td>
<td>Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>l2tp-tos-reflect</td>
<td>Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-tunnel-authen</td>
<td>If this attribute is set, it performs L2TP tunnel authentication. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-tunnel-password</td>
<td>Shared secret used for L2TP tunnel authentication and AVP hiding. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>l2tp-udp-checksum</td>
<td>This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>link-compression=</td>
<td>Defines whether to turn on or turn off “stac” compression over a PPP link. Used with service=ppp.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>Link compression is defined as a numeric value as follows:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1: Stac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2: Stac-Draft-9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3: MS-Stac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>load-threshold=&lt;n&gt;</td>
<td>Sets the load threshold for the caller at which additional links are either added to or deleted from the multilink bundle. If the load goes above the specified value, additional links are added. If the load goes below the specified value, links are deleted. Used with service=ppp and protocol=multilink. The range for &lt;n&gt; is from 1 to 255.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>map-class</td>
<td>Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out. Used with the service=outbound and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>max-links=&lt;n&gt;</td>
<td>Restricts the number of links that a user can have in a multilink bundle. Used with service=ppp and protocol=multilink. The range for &lt;n&gt; is from 1 to 255.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>min-links</td>
<td>Sets the minimum number of links for MLP. Used with service=ppp and protocol=multilink, protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>nas-password</td>
<td>Specifies the password for the network access server during the L2F tunnel authentication. Used with service=ppp and protocol=vpdn.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>nocallback-verify</td>
<td>Indicates that no callback verification is required. The only valid value for this parameter is 1 (for example, nocallback-verify=1). Used with service=arap, service=slip, service=ppp, service=shell. There is no authentication on callback. Not valid for ISDN.</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>noescape=x</td>
<td>Prevents user from using an escape character. Used with service=shell. Can be either true or false (for example, noescape=true).</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>nohangup=x</td>
<td>Used with service=shell. Specifies the nohangup option, which means that after an EXEC shell is terminated, the user is presented with another login (username) prompt. Can be either true or false (for example, nohangup=false).</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>old-prompts</td>
<td>Allows providers to make the prompts in TACACS+ appear identical to those of earlier systems (TACACS and Extended TACACS). This allows administrators to upgrade from TACACS or Extended TACACS to TACACS+ transparently to users.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>outacl#&lt;n&gt;</td>
<td>ASCII access list identifier for an interface output access list to be installed and applied to an interface for the duration of the current condition. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Per-user access lists do not currently work with ISDN interfaces.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>outacl=x</td>
<td>ASCII identifier for an interface output access list. Used with service=ppp and protocol=ip, and service service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must be preconfigured on the router. Per-user access lists do not currently work with ISDN interfaces.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>pool-def#&lt;n&gt;</td>
<td>Defines IP address pools on the network access server. Used with service=ppp and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>pool-timeout=</td>
<td>Defines (in conjunction with pool-def) IP address pools on the network access server. During IPCP address negotiation, if an IP pool name is specified for a user (see the addr-pool attribute), a check is made to see if the named pool is defined on the network access server. If it is, the pool is consulted for an IP address. Used with service=ppp and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
### Attribute Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>11.0</th>
<th>11.1</th>
<th>11.2</th>
<th>11.3</th>
<th>12.0</th>
<th>12.1</th>
<th>12.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-type</td>
<td>Indicates the type of physical port the network access server is using to authenticate the user. Physical ports are indicated by a numeric value as follows:</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>• 0: Asynchronous</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1: Synchronous</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2: ISDN-Synchronous</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3: ISDN-Asynchronous (V.120)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4: ISDN-Asynchronous (V.110)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5: Virtual</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used with service=any and protocol=aaa.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ppp-vj-slot-compression</td>
<td>Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>priv-lvl=x</td>
<td>Privilege level to be assigned for the EXEC. Used with service=shell. Privilege levels range from 0 to 15, with 15 being the highest.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>protocol=x</td>
<td>A protocol that is a subset of a service. An example would be any PPP NCP. Currently known values are lcp, ip, ipx, atalk, vines, lat, xremote, tn3270, telnet, rlogin, pad, vpdn, osicp, deccp, ccp, cdp, bridging, xns, nbf, bap, multilink, and unknown.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>proxyacl#&lt;n&gt;</td>
<td>Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces. Used with the service=shell and protocol=exec.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>route</td>
<td>Specifies a route to be applied to an interface. Used with service=slip, service=ppp, and protocol=ip.</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows:

```
route="dst_address mask [gateway]"
```

This indicates a temporary static route that is to be applied. The `dst_address`, `mask`, and `gateway` are expected to be in the usual dotted-decimal notation, with the same meanings as in the familiar `ip route` configuration command on a network access server.

If `gateway` is omitted, the peer’s address is the gateway. The route is expunged when the connection terminates.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>11.0</th>
<th>11.1</th>
<th>11.2</th>
<th>11.3</th>
<th>12.0</th>
<th>12.1</th>
<th>12.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>route#&lt;n&gt;</td>
<td>Like the route AV pair, this specifies a route to be applied to an interface, but these routes are numbered, allowing multiple routes to be applied. Used with service=ppp and protocol=ip, and service=ppp and protocol=ipx.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>routing=x</td>
<td>Specifies whether routing information is to be propagated to and accepted from this interface. Used with service=slip, service=ppp, and protocol=ip. Equivalent in function to the /routing flag in SLIP and PPP commands. Can either be true or false (for example, routing=true).</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>rte-fltr-in#&lt;n&gt;</td>
<td>Specifies an input access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>rte-fltr-out#&lt;n&gt;</td>
<td>Specifies an output access list definition to be installed and applied to routing updates on the current interface for the duration of the current connection. Used with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>sap#&lt;n&gt;</td>
<td>Specifies static Service Advertising Protocol (SAP) entries to be installed for the duration of a connection. Used with service=ppp and protocol=ipx.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>sap-fltr-in#&lt;n&gt;</td>
<td>Specifies an input SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>sap-fltr-out#&lt;n&gt;</td>
<td>Specifies an output SAP filter access list definition to be installed and applied on the current interface for the duration of the current connection. Used with service=ppp and protocol=ipx.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>send-auth</td>
<td>Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication. Used with service=any and protocol=aaa.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>send-secret</td>
<td>Specifies the password that the NAS needs to respond to a chap/pap request from the remote end of a connection on an outgoing call. Used with service=ppp and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>service=x</td>
<td>The primary service. Specifying a service attribute indicates that this is a request for authorization or accounting of that service. Current values are slip, ppp, arap, shell, tty-daemon, connection, and system. This attribute must always be included.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>source-ip=x</td>
<td>Used as the source IP address of all VPDN packets generated as part of a VPDN tunnel. This is equivalent to the Cisco vpdn outgoing global configuration command.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
### Attribute | Description | 11.0 | 11.1 | 11.2 | 11.3 | 12.0 | 12.1 | 12.2  
--- | --- | --- | --- | --- | --- | --- | --- | ---  
spi | Carries the authentication information needed by the home agent to authenticate a mobile node during registration. The information is in the same syntax as the `ip mobile secure host <addr>` configuration command. Basically it contains the rest of the configuration command that follows that string, verbatim. It provides the Security Parameter Index (SPI), key, authentication algorithm, authentication mode, and replay protection timestamp range. Used with the service=mobileip and protocol=ip. | no | no | no | no | no | yes | yes  
timeout=x | The number of minutes before an EXEC or ARA session disconnects (for example, timeout=60). A value of zero indicates no timeout. Used with service=arap. | yes | yes | yes | yes | yes | yes | yes  
tunnel-id | Specifies the username that will be used to authenticate the tunnel over which the individual user MID will be projected. This is analogous to the `remote name` in the `vpdn outgoing` command. Used with service=ppp and protocol=vpdn. | no | no | yes | yes | yes | yes | yes  
wins-servers= | Identifies a Windows NT server that can be requested by Microsoft PPP clients from the network access server during IPCP negotiation. To be used with service=ppp and protocol=ip. The IP address identifying each Windows NT server is entered in dotted decimal format. | no | no | no | yes | yes | yes | yes  
zonelist=x | A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5). | yes | yes | yes | yes | yes | yes | yes  

See Configuring TACACS+. module for the documents used to configure TACACS+, and TACACS+ authentication and authorization.

### TACACS Accounting AV Pairs

The following table lists and describes the supported TACACS+ accounting AV pairs and specifies the Cisco IOS release in which they are implemented.

#### Table 61: Supported TACACS+ Accounting AV Pairs

| Attribute   | Description                                                                 | 11.0 | 11.1 | 11.2 | 11.3 | 12.0 | 12.1 | 12.2  
|-------------|------------------------------------------------------------------------------|------|------|------|------|------|------|------  
Abort-Cause | If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server. | no   | no   | no   | no   | no   | yes  | yes  
bytes_in   | The number of input bytes transferred during this connection.                | yes  | yes  | yes  | yes  | yes  | yes  | yes  
bytes_out  | The number of output bytes transferred during this connection.               | yes  | yes  | yes  | yes  | yes  | yes  | yes  
Call-Type  | Describes the type of fax activity: fax receive or fax send.                 | no   | no   | no   | no   | no   | yes  | yes  
cmd        | The command the user executed.                                              | yes  | yes  | yes  | yes  | yes  | yes  | yes  

---
### TACACS Accounting AV Pairs

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>11.0</th>
<th>11.1</th>
<th>11.2</th>
<th>11.3</th>
<th>12.0</th>
<th>12.1</th>
<th>12.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>data-rate</td>
<td>This AV pair has been renamed. See nas-rx-speed.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>disc-cause</td>
<td>Specifies the reason a connection was taken off-line. The Disconnect-Cause attribute is sent in accounting-stop records. This attribute also causes stop records to be generated without first generating start records if disconnection occurs before authentication is performed. Refer to the following table (Disconnect Cause Extensions) for a list of Disconnect-Cause values and their meanings.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>disc-cause-ext</td>
<td>Extends the disc-cause attribute to support vendor-specific reasons why a connection was taken off-line.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>elapsed_time</td>
<td>The elapsed time in seconds for the action. Useful when the device does not keep real time.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Email-Server-Address</td>
<td>Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Email-Server-Ack-Flag</td>
<td>Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>event</td>
<td>Information included in the accounting packet that describes a state change in the router. Events described are accounting starting and accounting stopping.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Account-Id-Origin</td>
<td>Indicates the account ID origin as defined by system administrator for the mmoip aaa receive-id or the mmoip aaa send-id command.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Auth-Status</td>
<td>Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Connect-Speed</td>
<td>Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Coverpage-Flag</td>
<td>Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Dsn-Address</td>
<td>Indicates the address to which DSNs will be sent.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Dsn-Flag</td>
<td>Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Mdn-Address</td>
<td>Indicates the address to which MDNs will be sent.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Fax-Mdn-Flag</td>
<td>Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Fax-Modem-Time</td>
<td>Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Fax-Msg-Id=</td>
<td>Indicates a unique fax message identification number assigned by Store and Forward Fax.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Fax-Pages</td>
<td>Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Fax-Process-Abort-Flag</td>
<td>Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Fax-Recipient-Count</td>
<td>Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Gateway-Id</td>
<td>Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>mlp-links-max</td>
<td>Gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>mlp-sess-id</td>
<td>Reports the identification number of the multilink bundle when the session closes. This attribute applies to sessions that are part of a multilink bundle. This attribute is sent in authentication-response packets.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>nas-rx-speed</td>
<td>Specifies the average number of bits per second over the course of the connection’s lifetime. This attribute is sent in accounting-stop records.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>nas-tx-speed</td>
<td>Reports the transmit speed negotiated by the two modems.</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>paks_in</td>
<td>The number of input packets transferred during this connection.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>paks_out</td>
<td>The number of output packets transferred during this connection.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td>The port the user was logged in to.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Port-Used</td>
<td>Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>pre-bytes-in</td>
<td>Records the number of input bytes before authentication. This attribute is sent in accounting-stop records.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>pre-bytes-out</td>
<td>Records the number of output bytes before authentication. This attribute is sent in accounting-stop records.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>pre-paks-in</td>
<td>Records the number of input packets before authentication. This attribute is sent in accounting-stop records.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>pre-paks-out</td>
<td>Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>pre-session-time</td>
<td>Specifies the length of time, in seconds, from when a call first connects to when it completes authentication.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>priv_level</td>
<td>The privilege level associated with the action.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>protocol</td>
<td>The protocol associated with the action.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>reason</td>
<td>Information included in the accounting packet that describes the event that caused a system change. Events described are system reload, system shutdown, or when accounting is reconfigured (turned on or off).</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>service</td>
<td>The service the user used.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>start_time</td>
<td>The time the action started (in seconds since the epoch, 12:00 a.m. Jan 1 1970). The clock must be configured to receive this information.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>stop_time</td>
<td>The time the action stopped (in seconds since the epoch.) The clock must be configured to receive this information.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>task_id</td>
<td>Start and stop records for the same event must have matching (unique) task_id numbers.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>timezone</td>
<td>The time zone abbreviation for all timestamps included in this packet.</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>xmit-rate</td>
<td>This AV pair has been renamed. See nas-tx-speed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table lists the cause codes and descriptions for the Disconnect Cause Extended (disc-cause-ext) attribute.

**Table 62: Disconnect Cause Extensions**

<table>
<thead>
<tr>
<th>Cause Codes</th>
<th>Description</th>
<th>11.0</th>
<th>11.1</th>
<th>11.2</th>
<th>11.3</th>
<th>12.0</th>
<th>12.1</th>
<th>12.2</th>
<th>12.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 - No Reason</td>
<td>No reason for the disconnect.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1001 - No Disconnect</td>
<td>The event was not a disconnect.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1002 - Unknown</td>
<td>The reason for the disconnect is unknown. This code can appear when the remote connection goes down.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1003 - Call Disconnect</td>
<td>The call has disconnected.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1004 - CLID Auth Fail</td>
<td>Calling line ID (CLID) authentication has failed.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1009 - No Modem Available</td>
<td>The modem is not available.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1010 - No Carrier</td>
<td>The modem never detected data carrier detect (DCD). This code can appear if a disconnect occurs during the initial modem connection.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1011 - Lost Carrier</td>
<td>The modem detected DCD but became inactive. This code can appear if a disconnect occurs during the initial modem connection.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1012 - No Modem Results</td>
<td>The result codes could not be parsed. This code can appear if a disconnect occurs during the initial modem connection.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1020 - TS User Exit</td>
<td>The user exited normally from the terminal server. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1021 - Idle Timeout</td>
<td>The user exited from the terminal server because the idle timer expired. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1022 - TS Exit Telnet</td>
<td>The user exited normally from a Telnet session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1023 - TS No IP Addr</td>
<td>The user could not switch to Serial Line Internet Protocol (SLIP) or PPP because the remote host had no IP address or because the dynamic pool could not assign one. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1024 - TS TCP Raw Exit</td>
<td>The user exited normally from a raw TCP session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1025 - TS Bad Password</td>
<td>The login process ended because the user failed to enter a correct password after three attempts. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1026 - TS No TCP Raw</td>
<td>The raw TCP option is not enabled. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1027 - TS CNTL-C</td>
<td>The login process ended because the user typed Ctrl-C. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1028 - TS Session End</td>
<td>The terminal server session has ended. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1029 - TS Close Vconn</td>
<td>The user closed the virtual connection. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1030 - TS End Vconn</td>
<td>The virtual connection has ended. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1031 - TS Rlogin Exit</td>
<td>The user exited normally from an Rlogin session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1032 - TS Rlogin Opt Invalid</td>
<td>The user selected an invalid Rlogin option. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1033 - TS Insuff Resources</td>
<td>The access server has insufficient resources for the terminal server session. This code is related to immediate Telnet and raw TCP disconnects during a terminal server session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1040 - PPP LCP Timeout</td>
<td>PPP link control protocol (LCP) negotiation timed out while waiting for a response from a peer. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1041 - PPP LCP Fail</td>
<td>There was a failure to converge on PPP LCP negotiations. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1042 - PPP Pap Fail</td>
<td>PPP Password Authentication Protocol (PAP) authentication failed. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1043 - PPP CHAP Fail</td>
<td>PPP Challenge Handshake Authentication Protocol (CHAP) authentication failed. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1044 - PPP Remote Fail</td>
<td>Authentication failed from the remote server. This code concerns PPP sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1045 - PPP Receive Term</td>
<td>The peer sent a PPP termination request. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>PPP LCP Close (1046)</td>
<td>LCP got a close request from the upper layer while LCP was in an open state. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1047 - PPP No NCP</td>
<td>LCP closed because no NCPs were open. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1048 - PPP MP Error</td>
<td>LCP closed because it could not determine to which Multilink PPP bundle that it should add the user. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1049 - PPP Max Channels</td>
<td>LCP closed because the access server could not add any more channels to an MP session. This code concerns PPP connections.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1050 - TS Tables Full</td>
<td>The raw TCP or Telnet internal session tables are full. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1051 - TS Resource Full</td>
<td>Internal resources are full. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1052 - TS Invalid IP Addr</td>
<td>The IP address for the Telnet host is invalid. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1053 - TS Bad Hostname</td>
<td>The access server could not resolve the host name. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1054 - TS Bad Port</td>
<td>The access server detected a bad or missing port number. This code relates to immediate Telnet and raw TCP disconnects and contains more specific information than the Telnet and TCP codes listed earlier in this table.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1060 - TCP Reset</td>
<td>The host reset the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1061 - TCP Connection Refused</td>
<td>The host refused the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1062 - TCP Timeout</td>
<td>The TCP connection timed out. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1063 - TCP Foreign Host Close</td>
<td>A foreign host closed the TCP connection. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1064 - TCP Net Unreachable</td>
<td>The TCP network was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1065 - TCP Host Unreachable</td>
<td>The TCP host was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1066 - TCP Net Admin Unreachable</td>
<td>The TCP network was administratively unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1067 - TCP Host Admin Unreachable</td>
<td>The TCP host was administratively unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1068 - TCP Port Unreachable</td>
<td>The TCP port was unreachable. The TCP stack can return this disconnect code during an immediate Telnet or raw TCP session.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1100 - Session Timeout</td>
<td>The session timed out because there was no activity on a PPP link. This code applies to all session types.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1101 - Security Fail</td>
<td>The session failed for security reasons. This code applies to all session types.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1102 - Callback</td>
<td>The session ended for callback. This code applies to all session types.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1120 - Unsupported</td>
<td>One end refused the call because the protocol was disabled or unsupported. This code applies to all session types.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1150 - Radius Disc</td>
<td>The RADIUS server requested the disconnect.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1151 - Local Admin Disc</td>
<td>The local administrator has disconnected.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1152 - SNMP Disc</td>
<td>Simple Network Management Protocol (SNMP) has disconnected.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1160 - V110 Retries</td>
<td>The allowed retries for V110 synchronization have been exceeded.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1170 - PPP Auth Timeout</td>
<td>Authentication timeout. This code applies to PPP sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1180 - Local Hangup</td>
<td>The call disconnected as the result of a local hangup.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1185 - Remote Hangup</td>
<td>The call disconnected because the remote end hung up.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1190 - T1 Quiesced</td>
<td>The call disconnected because the T1 line that carried it was quiesced.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1195 - Call Duration</td>
<td>The call disconnected because the call duration exceeded the maximum amount of time allowed by the Max Call Mins or Max DS0 Mins parameter on the access server.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1600 - VPDN User Disconnect</td>
<td>The user disconnected. This value applies to virtual private dial-up network (VPDN) sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>1601 - VPDN Carrier Loss</td>
<td>Carrier loss has occurred. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1602 - VPDN No Resources</td>
<td>There are no resources. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1603 - VPDN Bad Control Packet</td>
<td>The control packet is invalid. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1604 - VPDN Admin Disconnect</td>
<td>The administrator disconnected. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1605 - VPDN Tunnel Down/Setup Fail</td>
<td>The tunnel is down or the setup failed. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1606 - VPDN Local PPP Disconnect</td>
<td>There was a local PPP disconnect. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1607 - VPDN Softshut/Session Limit</td>
<td>New sessions cannot be established on the VPN tunnel. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1608 - VPDN Call Redirected</td>
<td>The call was redirected. This code applies to VPDN sessions.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1801 - Q850 Unassigned Number</td>
<td>The number has not been assigned. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1802 - Q850 No Route</td>
<td>The equipment that is sending this code has received a request to route the call through a particular transit network that it does not recognize. The equipment that is sending this code does not recognize the transit network because either the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment that is sending this code. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1803 - Q850 No Route To Destination</td>
<td>The called party cannot be reached because the network through which the call has been routed does not serve the destination that is desired. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1806 - Q850 Channel Unacceptable</td>
<td>The channel that has been most recently identified is not acceptable to the sending entity for use in this call. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1816 - Q850 Normal Clearing</td>
<td>The call is being cleared because one of the users who is involved in the call has requested that the call be cleared. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>1817 - Q850 User Busy</td>
<td>The called party is unable to accept another call because the user-busy condition has been encountered. This code may be generated by the called user or by the network. In the case of the user, the user equipment is compatible with the call. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1818 - Q850 No User Responding</td>
<td>Used when a called party does not respond to a call-establishment message with either an alerting or connect indication within the prescribed period of time that was allocated. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1819 - Q850 No User Answer</td>
<td>The called party has been alerted but does not respond with a connect indication within a prescribed period of time. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1821 - Q850 Call Rejected</td>
<td>The equipment that is sending this code does not wish to accept this call although it could have accepted the call because the equipment that is sending this code is neither busy nor incompatible. This code may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1822 - Q850 Number Changed</td>
<td>The number that is indicated for the called party is no longer assigned. The new called party number may optionally be included in the diagnostic field. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1827 - Q850 Destination Out of Order</td>
<td>The destination that was indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term “not functioning correctly” indicates that a signaling message was unable to be delivered to the remote party. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1828 - Q850 Invalid Number Format</td>
<td>The called party cannot be reached because the called party number is not in a valid format or is not complete. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1829 - Q850 Facility Rejected</td>
<td>This code is returned when a supplementary service that was requested by the user cannot be provided by the network. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1830 - Q850 Responding to Status Enquiry</td>
<td>This code is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1831 - Q850 Unspecified Cause</td>
<td>No other code applies. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1834 - Q850 No Circuit Available</td>
<td>No circuit or channel is available to handle the call. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1838 - Q850 Network Out of Order</td>
<td>The network is not functioning correctly and the condition is likely to last a relatively long period of time. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1841 - Q850 Temporary Failure</td>
<td>The network is not functioning correctly and the condition is not likely to last a long period of time. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1842 - Q850 Network Congestion</td>
<td>The network is congested. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1843 - Q850 Access Info Discarded</td>
<td>This code indicates that the network could not deliver access information to the remote user as requested. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1844 - Q850 Requested Channel Not Available</td>
<td>This code is returned when the circuit or channel that is indicated by the requesting entity cannot be provided by the other side of the interface. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1845 - Q850 Call Pre-empted</td>
<td>The call was preempted. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1847 - Q850 Resource Unavailable</td>
<td>This code is used to report a resource-unavailable event only when no other code in the resource-unavailable class applies. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1850 - Q850 Facility Not Subscribed</td>
<td>Not a subscribed facility. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1852 - Q850 Outgoing Call Barred</td>
<td>Although the calling party is a member of the closed user group for the outgoing closed user group call, outgoing calls are not allowed for this member. This code applies to ISDN or modem calls that came in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Q850 Incoming Call Barred (1854)</td>
<td>Although the called party is a member of the closed user group for the incoming closed user group call, incoming calls are not allowed to this member. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1858 - Q850 Bearer Capability Not Available</td>
<td>The user has requested a bearer capability that is implemented by the equipment that generated this code but that is not available at this time. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1863 - Q850 Service Not Available</td>
<td>The code is used to report a service- or option-not-available event only when no other code in the service- or option-not-available class applies. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Cause Codes</td>
<td>Description</td>
<td>11.0</td>
<td>11.1</td>
<td>11.2</td>
<td>11.3</td>
<td>12.0</td>
<td>12.1</td>
<td>12.2</td>
<td>12.3</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>1865 - Q850 Bearer Capability Not Implemented</td>
<td>The equipment that is sending this code does not support the bearer capability that was requested. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1866 - Q850 Channel Not Implemented</td>
<td>The equipment that is sending this code does not support the channel type that was requested. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1869 - Q850 Facility Not Implemented</td>
<td>The supplementary service requested by the user cannot be provided by the network. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1881 - Q850 Invalid Call Reference</td>
<td>The equipment that is sending this code has received a message having a call reference that is not currently in use on the user-network interface. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1882 - Q850 Channel Does Not Exist</td>
<td>The channel most recently identified is not acceptable to the sending entity for use in this call. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1888 - Q850 Incompatible Destination</td>
<td>The equipment that is sending this code has received a request to establish a call that has low-layer compatibility or other compatibility attributes that cannot be accommodated. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1896 - Q850 Mandatory Info Element Is Missing</td>
<td>The equipment that is sending this code has received a message that is missing an information element that must be present in the message before that message can be processed. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1897 - Q850 Non Existent Message Type</td>
<td>The equipment that is sending this code has received a message with a message type that it does not recognize either because this is a message that is not defined or that is defined but not implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1898 - Q850 Invalid Message</td>
<td>This code is used to report an invalid message when no other code in the invalid message class applies. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1899 - Q850 Bad Info Element</td>
<td>The information element not recognized. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
**Cause Codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>11.0</th>
<th>11.1</th>
<th>11.2</th>
<th>11.3</th>
<th>12.0</th>
<th>12.1</th>
<th>12.2</th>
<th>12.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1900 - Q850 Invalid Element Contents</td>
<td>The equipment that is sending this code has received an information element that it has implemented; however, one or more fields in the information element are coded in such a way that has not been implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1901 - Q850 Wrong Message for State</td>
<td>The message that was received is incompatible with the call state. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1902 - Q850 Recovery on Timer Expiration</td>
<td>A procedure has been initiated by the expiration of a timer in association with error-handling procedures. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1903 - Q850 Info Element Error</td>
<td>The equipment that is sending this code has received a message that includes information elements or parameters that are not recognized because the information element identifiers or parameter names are not defined or are defined but not implemented by the equipment that is sending this code. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1911 - Q850 Protocol Error</td>
<td>This code is used to report a protocol error event only when no other code in the protocol error class applies. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>1927 - Q850 Unspecified Internetworking Event</td>
<td>There has been an error when interworking with a network that does not provide codes for actions that it takes. This code applies to ISDN or modem calls that have come in over ISDN.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Configuring AAA Server Group Selection Based on DNIS**

Cisco software allows you to authenticate users to a particular AAA server group based on the Dialed Number Identification Service (DNIS) number of the session. Any phone line (a regular home phone or a commercial T1/PRI line) can be associated with several phone numbers. The DNIS number identifies the number that was called to reach you.

For example, suppose you want to share the same phone number with several customers, but you want to know which customer is calling before you pick up the phone. You can customize how you answer the phone because DNIS allows you to know which customer is calling when you answer.

Cisco devices with either ISDN or internal modems can receive the DNIS number. This functionality allows users to assign different TACACS+ server groups for different customers (that is, different TACACS+ servers for different DNIS numbers). Additionally, using server groups you can specify the same server group for AAA services or a separate server group for each AAA service.

Cisco IOS software provides the flexibility to implement authentication and accounting services in several ways:
• Globally--AAA services are defined using global configuration access list commands and applied in
general to all interfaces on a specific network access server.

• Per interface--AAA services are defined using interface configuration commands and applied specifically
to the interface being configured on a specific network access server.

• DNIS mapping--You can use DNIS to specify an AAA server to supply AAA services.

Because AAA configuration methods can be configured simultaneously, Cisco has established an order of
precedence to determine which server or groups of servers provide AAA services. The order of precedence
is as follows:

• Per DNIS--If you configure the network access server to use DNIS to identify which server group provides
AAA services, then this method takes precedence over any additional AAA selection method.

• Per interface--If you configure the network access server per interface to use access lists to determine
how a server provides AAA services, this method takes precedence over any global configuration AAA
access lists.

• Globally--If you configure the network access server by using global AAA access lists to determine how
the security server provides AAA services, this method has the lowest precedence.

Prior to configuring AAA Server Group Selection Based on DNIS, you must configure the remote security
servers associated with each AAA server group. See Identifying the TACACS Server Host and Configuring
AAA Server Groups for more information.

To configure the device to select a particular AAA server group based on the DNIS of the server group,
configure DNIS mapping. To map a server group with a group name with DNIS number, use the following
commands in global configuration mode:

**SUMMARY STEPS**

1. Device>enable
2. Device#configure terminal
3. Device(config)#aaa dnis map enable
4. Router(config)# aaa dnis map dnis-number authentication ppp group server-group-name
5. Router(config)# aaa dnis map dnis-number accounting network [none | start-stop | stop-only] group server-group-name

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Device&gt;enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Device#configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Device (config)#aaa dnis map enable</td>
<td>Enables DNIS mapping.</td>
</tr>
</tbody>
</table>
### TACACS+ Configuration Options

You can configure the switch to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

### TACACS+ Login Authentication

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

### TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user’s profile, which is located either in the local user database or on the security server, to configure the user’s session. The user is granted access to a requested service only if the information in the user profile allows it.

### TACACS+ Authentication

After you have identified the TACACS+ daemon and defined an associated TACACS+ encryption key, you must define method lists for TACACS+ authentication. Because TACACS+ authentication is operated via AAA, you need to issue the `aaa authentication` command, specifying TACACS+ as the authentication method.

### TACACS+ Authorization

AAA authorization enables you to set parameters that restrict a user’s access to the network. Authorization via TACACS+ may be applied to commands, network connections, and EXEC sessions. Because TACACS+ authorization is facilitated through AAA, you must issue the `aaa authorization` command, specifying TACACS+ as the authorization method.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# <code>aaa dnis map dnis-number authentication ppp group server-group-name</code></td>
<td>Maps a DNIS number to a defined AAA server group; the servers in this server group are being used for authentication.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# `aaa dnis map dnis-number accounting network [none</td>
<td>start-stop</td>
</tr>
</tbody>
</table>
TACACS+ Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the switch reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

Note

Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

Per VRF for TACACS Servers

The Per VRF for TACACS+ Servers feature allows per virtual routing and forwarding (VRF) AAA to be configured on TACACS+ servers. TACACS+ server access is required to configure this feature.

How to Configure TACACS+

Identifying the TACACS+ Server Host and Setting the Authentication Key

Follow these steps to identify the TACACS+ server host and set the authentication key:

SUMMARY STEPS

1. enable
2. configure terminal
3. tacacs-server host hostname
4. aaa new-model
5. aaa group server tacacs+ group-name
6. server ip-address
7. end
8. show running-config
9. copy running-config startup-config
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode.                                      |
| Example:                     |                                                                         |
| Switch# configure terminal   |                                                                         |

| **Step 3** tacacs-server host hostname | Identifies the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. For hostname, specify the name or IP address of the host. |
| Example:                        |                                                                         |
| Switch(config)# tacacs-server host yourserver |                                                                         |

| **Step 4** aaa new-model      | Enables AAA.                                                           |
| Example:                      |                                                                         |
| Switch(config)# aaa new-model |                                                                         |

| **Step 5** aaa group server tacacs+ group-name | (Optional) Defines the AAA server-group with a group name. This command puts the Switch in a server group subconfiguration mode. |
| Example:                                  |                                                                         |
| Switch(config)# aaa group server tacacs+ your_server_group |                                                                         |

| **Step 6** server ip-address | (Optional) Associates a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 3. |
| Example:                     |                                                                         |
| Switch(config)# server 10.1.2.3 |                                                                         |

| **Step 7** end               | Returns to privileged EXEC mode.                                       |
| Example:                     |                                                                         |
| Switch(config)# end          |                                                                         |

| **Step 8** show running-config | Verifies your entries.                                                 |
| Example:                      |                                                                         |
### Configuring TACACS+ Login Authentication

Follow these steps to configure TACACS+ login authentication:

**Before you begin**

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports.

**Note**

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

For more information about the `ip http authentication` command, see the *Cisco IOS Security Command Reference, Release 12.4*.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication login {default | list-name} method1 [method2...]`
5. `line [console | tty | vty] line-number [ending-line-number]`
6. `login authentication {default | list-name}`
7. `end`
8. `show running-config`
9. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa authentication login {default</td>
<td>list-name} method1 [method2...]</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# aaa authentication login default tacacs+ local</td>
<td></td>
</tr>
</tbody>
</table>

- To create a default list that is used when a named list is *not* specified in the `login authentication` command, use the `default` keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.
- For `list-name`, specify a character string to name the list you are creating.
- For `method1...`, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Select one of these methods:

- **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the `enable password` global configuration command.
- **group tacacs+**—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. For more information, see the Identifying the TACACS+ Server Host and Setting the Authentication Key, on page 521.
- **line**—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the `password password` line configuration command.
- **local**—Use the local username database for authentication. You must enter username information in the database. Use the `username password` global configuration command.
- **local-case**—Use a case-sensitive local username database for authentication. You must enter username
### Command or Action | Purpose
---|---
| information in the database by using the `username name password` global configuration command. | • *none*—Do not use any authentication for login.

**Step 5**

`line [console | tty | vty] line-number [ending-line-number]`  
**Example:**  
`Switch(config)# line 2 4`  

Enters line configuration mode, and configures the lines to which you want to apply the authentication list.

**Step 6**

`login authentication {default | list-name}`  
**Example:**  
`Switch(config-line)# login authentication default`  

Applies the authentication list to a line or set of lines.  
• If you specify `default`, use the default list created with the `aaa authentication login` command.  
• For `list-name`, specify the list created with the `aaa authentication login` command.

**Step 7**

`end`  
**Example:**  
`Switch(config-line)# end`  

Returns to privileged EXEC mode.

**Step 8**

`show running-config`  
**Example:**  
`Switch# show running-config`  

Verifies your entries.

**Step 9**

`copy running-config startup-config`  
**Example:**  
`Switch# copy running-config startup-config`  

(Optional) Saves your entries in the configuration file.

---

### Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

You can use the `aaa authorization` global configuration command with the `tacacs+` keyword to set parameters that restrict a user’s network access to privileged EXEC mode.

**Note**  
Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.
Follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa authorization network tacacs+`
4. `aaa authorization exec tacacs+`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
| Example: Switch> `enable` | • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
| Example: Switch# `configure terminal` | |
| **Step 3** aaa authorization network tacacs+ | Configures the switch for user TACACS+ authorization for all network-related service requests.  
| Example: Switch(config)# `aaa authorization network tacacs+` | |
| **Step 4** aaa authorization exec tacacs+ | Configures the switch for user TACACS+ authorization if the user has privileged EXEC access.  
| Example: Switch(config)# `aaa authorization exec tacacs+` | The `exec` keyword might return user profile information (such as `autocommand` information). |
| **Step 5** end | Returns to privileged EXEC mode.  
| Example: Switch(config)# `end` | |
| **Step 6** show running-config | Verifies your entries.  
| Example: | |
Starting TACACS+ Accounting

Follow these steps to start TACACS+ Accounting:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa accounting network start-stop tacacs+
4. aaa accounting exec start-stop tacacs+
5. end
6. show running-config
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa accounting network start-stop tacacs+</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa accounting network start-stop tacacs+</td>
</tr>
<tr>
<td></td>
<td>Enables TACACS+ accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>aaa accounting exec start-stop tacacs+</td>
<td>Enables TACACS+ accounting to send a start-record accounting notice at</td>
</tr>
<tr>
<td>Example:</td>
<td>the beginning of a privileged EXEC process and a stop-record at the end.</td>
</tr>
<tr>
<td>Switch(config)# aaa accounting exec</td>
<td></td>
</tr>
<tr>
<td>start-stop tacacs+</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

To establish a session with a router if the AAA server is unreachable, use the `aaa accounting system guarantee-first` command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.

**Establishing a Session with a Router if the AAA Server is Unreachable**

To establishing a session with a router if the AAA server is unreachable, use the `aaa accounting system guarantee-first` command. It guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.
### Establishing a Session with a Router if the AAA Server is Unreachable

The `aaa accounting system guarantee-first` command guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.

To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.

### Configuring Per VRF on a TACACS Server

The initial steps in this procedure are used to configure AAA and a server group, create a VRF routing table, and configure an interface. Steps 10 through 13 are used to configure the per VRF on a TACACS+ server feature:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip vrf vrf-name`
4. `rd route-distinguisher`
5. `exit`
6. `interface interface-name`
7. `ip vrf forwarding vrf-name`
8. `ip address ip-address mask [secondary]`
9. `exit`
10. `aaa group server tacacs+ group-name`
11. `server-private {ip-address | name} [nat] [single-connection] [port port-number] [timeout seconds] [key [0 | 7] string]
12. `ip vrf forwarding vrf-name`
13. `ip tacacs source-interface subinterface-name`
14. `exit`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td><em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip vrf vrf-name</code></td>
<td>Configures a VRF table and enters VRF configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4** 
Device(config)# ip vrf cisco | Creates routing and forwarding tables for a VRF instance. |
| **Step 5** 
Device(config-vrf)# rd 100:1 | Exits VRF configuration mode. |
| **Step 6** 
Device(config-vrf)# exit | Exits VRF configuration mode. |
| **Step 7** 
Device(config-if)# ip vrf forwarding cisco | Configures a VRF for the interface. |
| **Step 8** 
Device(config-if)# ip address 10.0.0.2 255.0.0.0 | Sets a primary or secondary IP address for an interface. |
| **Step 9** 
Device(config-if)# exit | Exits interface configuration mode. |
| **Step 10** 
Device(config)# aaa group server tacacs+ tacacs1 | Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode. |
| **Step 11** 
Device(config-sg-tacacs+)# server-private10.1.1.1 port 19 key cisco | Configures the IP address of the private TACACS+ server for the group server. |
| **Step 12** 
Device(config-if)# ip vrf forwarding cisco | Configures the VRF reference of a AAA TACACS+ server group. |
Purpose
Command or Action

Device(config-sg-tacacs+)# ip vrf forwarding cisco

Step 13
ip tacacs source-interface  subinterface-name
Example:
Device(config-sg-tacacs+)# ip tacacs source-interface Loopback0

Step 14
exit
Example:
Device(config-sg-tacacs)# exit

Verifying Per VRF for TACACS Servers

To verify the per VRF TACACS+ configuration, perform the following steps:

Note
The `debug` commands may be used in any order.

SUMMARY STEPS

1. enable
2. debug tacacs authentication
3. debug tacacs authorization
4. debug tacacs accounting
5. debug tacacs packets

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 debug tacacs authentication</td>
<td>Displays information about AAA/TACACS+ authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# debug tacacs authentication</td>
<td></td>
</tr>
<tr>
<td>Step 3 debug tacacs authorization</td>
<td>Displays information about AAA/TACACS+ authorization.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring TACACS+

#### Table 63: Commands for Displaying TACACS+ Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs</td>
<td>Displays TACACS+ server statistics.</td>
</tr>
</tbody>
</table>

### Configuration Examples for TACACS+

#### Example: TACACS Authorization

The following example shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure network authorization via TACACS+:

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
  ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.
• The **aaa authorization** command configures network authorization via TACACS+. Unlike authentication lists, this authorization list always applies to all incoming network connections made to the network access server.

• The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”

• The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

**Example: TACACS Accounting**

The following example shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure accounting via TACACS+:

```plaintext
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
    ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

• The **aaa new-model** command enables the AAA security services.

• The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

• The **aaa accounting** command configures network accounting via TACACS+. In this example, accounting records describing the session that just terminated will be sent to the TACACS+ daemon whenever a network connection terminates.

• The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”

• The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

**Example: TACACS Authentication**

The following example shows how to configure TACACS+ as the security protocol for PPP authentication:

```plaintext
aaa new-model
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
```
The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.

- The **aaa authentication** command defines a method list, “test,” to be used on serial interfaces running PPP. The keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”

- The **interface** command selects the line, and the **ppp authentication** command applies the test method list to this line.

The following example shows how to configure TACACS+ as the security protocol for PPP authentication, but instead of the “test” method list, the “default” method list is used.

```plaintext
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
    tacacs-server host 10.1.2.3
    tacacs-server key goaway
    interface serial 0
    ppp authentication chap default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.

- The **aaa authentication** command defines a method list, “default,” to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”

- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The following example shows how to create the same authentication algorithm for PAP, but it calls the method list “MIS-access” instead of “default”:

```plaintext
aaa new-model
aaa authentication pap MIS-access if-needed group tacacs+ local
    tacacs-server host 10.1.2.3
    tacacs-server key goaway
    interface serial 0
    ppp authentication pap MIS-access
```
The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.

- The **aaa authentication** command defines a method list, “MIS-access,” to be used on serial interfaces running PPP. The method list, “MIS-access,” means that PPP authentication is applied to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, then PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the network access server.

- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key to be “goaway.”

- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The following example shows the configuration for a TACACS+ daemon with an IP address of 10.2.3.4 and an encryption key of “apple”:

```plaintext
aaa new-model
aaa authentication login default group tacacs+ local
  tacacs-server host 10.2.3.4
  tacacs-server key apple
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.

- The **aaa authentication** command defines the default method list. Incoming ASCII logins on all interfaces (by default) will use TACACS+ for authentication. If no TACACS+ server responds, then the network access server will use the information contained in the local username database for authentication.

- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.2.3.4. The **tacacs-server key** command defines the shared encryption key to be “apple.”

**Example: Configuring Per VRF for TACACS Servers**

The following output example shows that the group server **tacacs1** is configured for per VRF AAA services:

```plaintext
aaa group server tacacs+ tacacs1
  server-private 10.1.1.1 port 19 key cisco
  ip vrf forwarding cisco
  ip tacacs source-interface Loopback0
  ip vrf cisco
  rd 100:1
  interface Loopback0
    ip address 10.0.0.2 255.0.0.0
    ip vrf forwarding cisco
```
# Additional References for TACACS+

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Cisco security commands</td>
<td>• Cisco IOS Security Command Reference: Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
<tr>
<td>IPv6 commands</td>
<td>Cisco IOS IPv6 Command Reference</td>
</tr>
</tbody>
</table>

## MIBs

<table>
<thead>
<tr>
<th>MB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature Information for TACACS+

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
<tr>
<td>Cisco IOS 12.2(54)SG</td>
<td>The Per VRF for TACACS+ Servers feature allows per virtual route forwarding (per VRF) to be configured for authentication, authorization, and accounting (AAA) on TACACS+ servers.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(1)E</td>
<td>The following commands were introduced or modified: <code>ip tacacs source-interface</code>, <code>ip vrf forwarding</code> (server-group), <code>server-private</code> (TACACS+).</td>
</tr>
</tbody>
</table>
Feature Information for TACACS+
Configuring RADIUS

The RADIUS security system is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

- Finding Feature Information, on page 539
- Prerequisites for Configuring RADIUS, on page 539
- Restrictions for Configuring RADIUS, on page 540
- Information about RADIUS, on page 540
- How to Configure RADIUS, on page 560
- Configuration Examples for RADIUS, on page 575
- Additional References for RADIUS, on page 578
- Feature Information for RADIUS, on page 580

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring RADIUS

This section lists the prerequisites for controlling Switch access with RADIUS.

General:

- RADIUS and Authentication, Authorization, and Accounting (AAA) must be enabled to use any of the configuration commands in this chapter.

- RADIUS is facilitated through AAA and can be enabled only through AAA commands.

- Use the `aaa new-model` global configuration command to enable AAA.
• Use the `aaa authentication` global configuration command to define method lists for RADIUS authentication.

• Use `line` and `interface` commands to enable the defined method lists to be used.

• At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

• You should have access to and should configure a RADIUS server before configuring RADIUS features on your Switch.

• The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.

• To use the Change-of-Authorization (CoA) interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.

For RADIUS operation:

• Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled.

### Restrictions for Configuring RADIUS

This topic covers restrictions for controlling Switch access with RADIUS.

**General:**

• To prevent a lapse in security, you cannot configure RADIUS through a network management application.

RADIUS is not suitable in the following network security situations:

• Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.

• Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.

• Networks using a variety of services. RADIUS generally binds a user to one service model.

### Information about RADIUS

**RADIUS and Switch Access**

This section describes how to enable and configure RADIUS. RADIUS provides detailed accounting information and flexible administrative control over the authentication and authorization processes.
RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

Use RADIUS in these network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors’ access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.

- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma’s security cards to validates users and to grant access to network resources.

- Networks already using RADIUS. You can add a Cisco Switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 2: Transitioning from RADIUS to TACACS+ Services below.

- Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1x. For more information about this protocol, see Chapter 11, “Configuring IEEE 802.1x Port-Based Authentication.”

- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

Figure 44: Transitioning from RADIUS to TACACS+ Services

RADIUS Operation

When a user attempts to log in and authenticate to a Switch that is access controlled by a RADIUS server, these events occur:
1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   - ACCEPT—The user is authenticated.
   - REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   - CHALLENGE—A challenge requires additional data from the user.
   - CHALLENGE PASSWORD—A response requests the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. The additional data included with the ACCEPT or REJECT packets includes these items:

   - Telnet, SSH, rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and user timeouts

**Default RADIUS Configuration**

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the switch through the CLI.

**RADIUS Server Host**

Switch-to-RADIUS-server communication involves several components:

   - Hostname or IP address
   - Authentication destination port
   - Accounting destination port
   - Key string
   - Timeout period
   - Retransmission value

You identify RADIUS security servers by their hostname or IP address, hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the %RADIUS-4-RADIUS_DEAD message appears,
and then the switch tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the switch use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the switch.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings.

RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list. The default method list is automatically applied to all ports except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

AAA Server Groups

You can configure the switch to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If you configure two different host entries on the same RADIUS server for the same service, (for example, accounting), the second configured host entry acts as a fail-over backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

AAA Authorization

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user’s profile, which is in the local user database or on the security server, to configure the user’s session. The user is granted access to a requested service only if the information in the user profile allows it.
RADIUS Accounting

The AAA accounting feature tracks the services that users are using and the amount of network resources that they are consuming. When you enable AAA accounting, the switch reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. You can then analyze the data for network management, client billing, or auditing.

Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco’s vendor-ID is 9, and the supported option has vendor-type 1, which is named cisco-avpair. The value is a string with this format:

```
protocol : attribute sep value *
```

*Protocol* is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

For example, the following AV pair causes Cisco’s “multiple named IP address pools” feature to be activated during IP authorization (during PPP’s Internet Protocol Control Protocol (IPCP) address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

If you insert an “*”, the AV pair “ip:addr-pool=first” becomes optional. Note that any AV pair can be made optional:

```
cisco-avpair= "ip:addr-pool*first"
```

The following example shows how to cause a user logging in from a network access server to have immediate access to EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, “Remote Authentication Dial-In User Service (RADIUS).”

Attribute 26 contains the following three elements:

- Type
- Length
- String (also known as data)
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data
The figure below shows the packet format for a VSA encapsulated “behind” attribute 26.

**Figure 45: VSA Encapsulated Behind Attribute 26**

```
0 8 16 24
012345670123456701234567

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Vendor-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor-id</td>
<td>Vendor-type</td>
<td>Vendor-length</td>
</tr>
<tr>
<td>Attributes-specific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(vendor-data)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Note**

It is up to the vendor to specify the format of their VSA. The Attribute-Specific field (also known as Vendor-Data) is dependent on the vendor's definition of that attribute.

The table below describes significant fields listed in the Vendor-Specific RADIUS IETF Attributes table (second table below), which lists supported vendor-specific RADIUS attributes (IETF attribute 26).

**Table 64: Vendor-Specific Attributes Table Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>All attributes listed in the following table are extensions of IETF attribute 26.</td>
</tr>
<tr>
<td>Vendor-Specific Command Codes</td>
<td>A defined code used to identify a particular vendor. Code 9 defines Cisco VSAs, 311 defines Microsoft VSAs, and 529 defines Ascend VSAs.</td>
</tr>
<tr>
<td>Sub-Type Number</td>
<td>The attribute ID number. This number is much like the ID numbers of IETF attributes, except it is a “second layer” ID number encapsulated behind attribute 26.</td>
</tr>
<tr>
<td>Attribute</td>
<td>The ASCII string name of the attribute.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the attribute.</td>
</tr>
</tbody>
</table>

**Table 65: Vendor-Specific RADIUS IETF Attributes**

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-CHAP Attributes</td>
<td></td>
<td></td>
<td>MSCHAP-Response</td>
<td>Contains the response value provided by a PPP MS-CHAP user in response to the challenge. It is only used in Access-Request packets. This attribute is identical to the PPP CHAP Identifier. <em>(RFC 2548)</em></td>
</tr>
<tr>
<td>26</td>
<td>311</td>
<td>1</td>
<td>MSCHAP-Response</td>
<td></td>
</tr>
</tbody>
</table>
Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>311</td>
<td>11</td>
<td>MSCHAP-Challenge</td>
<td>Contains the challenge sent by a network access server to an MS-CHAP user. It can be used in both Access-Request and Access-Challenge packets. (RFC 2548)</td>
</tr>
</tbody>
</table>

VPDN Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-cm-local-window-size</td>
<td>Specifies the maximum receive window size for L2TP control messages. This value is advertised to the peer during tunnel establishment.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-drop-out-of-order</td>
<td>Respects sequence numbers on data packets by dropping those that are received out of order. This does not ensure that sequence numbers will be sent on data packets, just how to handle them if they are received.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-hello-interval</td>
<td>Specifies the number of seconds for the hello keepalive interval. Hello packets are sent when no data has been sent on a tunnel for the number of seconds configured here.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-hidden-avp</td>
<td>When enabled, sensitive AVPs in L2TP control messages are scrambled or hidden.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-nosession-timeout</td>
<td>Specifies the number of seconds that a tunnel will stay active with no sessions before timing out and shutting down.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>----------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>tunnel-tos-reflect</td>
<td>Copies the IP ToS field from the IP header of each payload packet to the IP header of the tunnel packet for packets entering the tunnel at the LNS.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-tunnel-authen</td>
<td>If this attribute is set, it performs L2TP tunnel authentication.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-tunnel-password</td>
<td>Shared secret used for L2TP tunnel authentication and AVP hiding.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>l2tp-udp-checksum</td>
<td>This is an authorization attribute and defines whether L2TP should perform UDP checksums for data packets. Valid values are “yes” and “no.” The default is no.</td>
</tr>
</tbody>
</table>

### Store and Forward Fax Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>3</td>
<td>Fax-Account-Id-Origin</td>
<td>Indicates the account ID origin as defined by system administrator for the <code>mnoip aaa receive-id</code> or the <code>mnoip aaa send-id</code> commands.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>4</td>
<td>Fax-Msg-Id</td>
<td>Indicates a unique fax message identification number assigned by Store and Forward Fax.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>5</td>
<td>Fax-Pages</td>
<td>Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>6</td>
<td>Fax-Coverpage-Flag</td>
<td>Indicates whether or not a cover page was generated by the off-ramp gateway for this fax session. True indicates that a cover page was generated; false means that a cover page was not generated.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>7</td>
<td>Fax-Modem-Time</td>
<td>Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>8</td>
<td>Fax-Connect-Speed</td>
<td>Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>9</td>
<td>Fax-Recipient-Count</td>
<td>Indicates the number of recipients for this fax transmission. Until e-mail servers support Session mode, the number should be 1.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>10</td>
<td>Fax-Process-Abort-Flag</td>
<td>Indicates that the fax session was aborted or successful. True means that the session was aborted; false means that the session was successful.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>11</td>
<td>Fax-Dsn-Address</td>
<td>Indicates the address to which DSNs will be sent.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>12</td>
<td>Fax-Dsn-Flag</td>
<td>Indicates whether or not DSN has been enabled. True indicates that DSN has been enabled; false means that DSN has not been enabled.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>13</td>
<td>Fax-Mdn-Address</td>
<td>Indicates the address to which MDNs will be sent.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>14</td>
<td>Fax-Mdn-Flag</td>
<td>Indicates whether or not message delivery notification (MDN) has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>15</td>
<td>Fax-Auth-Status</td>
<td>Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>16</td>
<td>Email-Server-Address</td>
<td>Indicates the IP address of the e-mail server handling the on-ramp fax-mail message.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>17</td>
<td>Email-Server-Ack-Flag</td>
<td>Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>18</td>
<td>Gateway-Id</td>
<td>Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>19</td>
<td>Call-Type</td>
<td>Describes the type of fax activity: fax receive or fax send.</td>
</tr>
</tbody>
</table>
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>20</td>
<td>Port-Used</td>
<td>Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>21</td>
<td>Abort-Cause</td>
<td>If the fax session aborts, indicates the system component that signaled the abort. Examples of system components that could trigger an abort are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server.</td>
</tr>
</tbody>
</table>

### H323 Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>23</td>
<td>Remote-Gateway-ID (h323-remote-address)</td>
<td>Indicates the IP address of the remote gateway.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>24</td>
<td>Connection-ID (h323-conf-id)</td>
<td>Identifies the conference ID.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>25</td>
<td>Setup-Time (h323-setup-time)</td>
<td>Indicates the setup time for this connection in Coordinated Universal Time (UTC) formerly known as Greenwich Mean Time (GMT) and Zulu time.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>26</td>
<td>Call-Origin (h323-call-origin)</td>
<td>Indicates the origin of the call relative to the gateway. Possible values are originating and terminating (answer).</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>27</td>
<td>Call-Type (h323-call-type)</td>
<td>Indicates call leg type. Possible values are telephony and VoIP.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>28</td>
<td>Connect-Time (h323-connect-time)</td>
<td>Indicates the connection time for this call leg in UTC.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>29</td>
<td>Disconnect-Time (h323-disconnect-time)</td>
<td>Indicates the time this call leg was disconnected in UTC.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>30</td>
<td>Disconnect-Cause (h323-disconnect-cause)</td>
<td>Specifies the reason a connection was taken offline per Q.931 specification.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>31</td>
<td>Voice-Quality (h323-voice-quality)</td>
<td>Specifies the impairment factor (ICPIF) affecting voice quality for a call.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>33</td>
<td>Gateway-ID (h323-gw-id)</td>
<td>Indicates the name of the underlying gateway.</td>
</tr>
</tbody>
</table>

### Large Scale Dialout Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>callback-dialstring</td>
<td>Defines a dialing string to be used for callback.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>data-service</td>
<td>No description available.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>dial-number</td>
<td>Defines the number to dial.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>force-56</td>
<td>Determines whether the network access server uses only the 56 K portion of a channel, even when all 64 K appear to be available.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>map-class</td>
<td>Allows the user profile to reference information configured in a map class of the same name on the network access server that dials out.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-auth</td>
<td>Defines the protocol to use (PAP or CHAP) for username-password authentication following CLID authentication.</td>
</tr>
<tr>
<td>Number</td>
<td>Vendor-Specific Company Code</td>
<td>Sub-Type Number</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-name</td>
<td>PPP name authentication. To apply for PAP, do not configure the <code>ppp pap send-name password</code> command on the interface. For PAP, “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For CHAP, “preauth:send-name” will be used not only for outbound authentication, but also for inbound authentication. For a CHAP inbound case, the NAS will use the name defined in “preauth:send-name” in the challenge packet to the caller box.</td>
</tr>
</tbody>
</table>

**Note**  
The send-name attribute has changed over time: Initially, it performed the functions now provided by both the send-name and remote-name attributes. Because the remote-name attribute has been added, the send-name attribute is restricted to its current behavior.
<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>send-secret</td>
<td>PPP password authentication. The vendor-specific attributes (VSAs) “preauth:send-name” and “preauth:send-secret” will be used as the PAP username and PAP password for outbound authentication. For a CHAP outbound case, both “preauth:send-name” and “preauth:send-secret” will be used in the response packet.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>remote-name</td>
<td>Provides the name of the remote host for use in large-scale dial-out. Dialer checks that the large-scale dial-out remote name matches the authenticated name, to protect against accidental user RADIUS misconfiguration. (For example, dialing a valid phone number but connecting to the wrong device.)</td>
</tr>
</tbody>
</table>

Miscellaneous Attributes
### Vendor-Specific RADIUS Attributes

<table>
<thead>
<tr>
<th>Number</th>
<th>Vendor-Specific Company Code</th>
<th>Sub-Type Number</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>9</td>
<td>2</td>
<td>Cisco-NAS-Port</td>
<td>Specifies additional vendor specific attribute (VSA) information for NAS-Port accounting. To specify additional NAS-Port information in the form an Attribute-Value Pair (AVPair) string, use the <code>radius-server vsa send</code> global configuration command. <strong>Note</strong> This VSA is typically used in Accounting, but may also be used in Authentication (Access-Request) packets.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>min-links</td>
<td>Sets the minimum number of links for MLP.</td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>1</td>
<td>proxyacl#&lt;n&gt;</td>
<td>Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.</td>
</tr>
</tbody>
</table>
RADIUS Disconnect-Cause Attribute Values

Disconnect-cause attribute values specify the reason a connection was taken offline. The attribute values are sent in Accounting request packets. These values are sent at the end of a session, even if the session fails to be authenticated. If the session is not authenticated, the attribute can cause stop records to be generated without first generating start records.

The table below lists the cause codes, values, and descriptions for the Disconnect-Cause (195) attribute.

<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No-Reason</td>
<td>No reason is given for the disconnect.</td>
</tr>
<tr>
<td>1</td>
<td>No-Disconnect</td>
<td>The event was not disconnected.</td>
</tr>
<tr>
<td>2</td>
<td>Unknown</td>
<td>Reason unknown.</td>
</tr>
<tr>
<td>3</td>
<td>Call-Disconnect</td>
<td>The call has been disconnected.</td>
</tr>
<tr>
<td>4</td>
<td>CLID-Authentication-Failure</td>
<td>Failure to authenticate number of the calling-party.</td>
</tr>
</tbody>
</table>

Note:
The Disconnect-Cause is incremented by 1000 when it is used in RADIUS AVPairs; for example, disc-cause 4 becomes 1004.
<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>No-Modem-Available</td>
<td>A modem in not available to connect the call.</td>
</tr>
<tr>
<td>10</td>
<td>No-Carrier</td>
<td>No carrier detected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Codes 10, 11, and 12 can be sent if there is a disconnection during initial modem connection.</td>
</tr>
<tr>
<td>11</td>
<td>Lost-Carrier</td>
<td>Loss of carrier.</td>
</tr>
<tr>
<td>12</td>
<td>No-Detected-Result-Codes</td>
<td>Failure to detect modem result codes.</td>
</tr>
<tr>
<td>20</td>
<td>User-Ends-Session</td>
<td>User terminates a session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Codes 20, 22, 23, 24, 25, 26, 27, and 28 apply to EXEC sessions.</td>
</tr>
<tr>
<td>21</td>
<td>Idle-Timeout</td>
<td>Timeout waiting for user input.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Codes 21, 100, 101, 102, and 120 apply to all session types.</td>
</tr>
<tr>
<td>22</td>
<td>Exit-Telnet-Session</td>
<td>Disconnect due to exiting Telnet session.</td>
</tr>
<tr>
<td>23</td>
<td>No-Remote-IP-Addr</td>
<td>Could not switch to SLIP/PPP; the remote end has no IP address.</td>
</tr>
<tr>
<td>24</td>
<td>Exit-Raw-TCP</td>
<td>Disconnect due to exiting raw TCP.</td>
</tr>
<tr>
<td>25</td>
<td>Password-Fail</td>
<td>Bad passwords.</td>
</tr>
<tr>
<td>26</td>
<td>Raw-TCP-Disabled</td>
<td>Raw TCP disabled.</td>
</tr>
<tr>
<td>27</td>
<td>Control-C-Detected</td>
<td>Control-C detected.</td>
</tr>
<tr>
<td>28</td>
<td>EXEC-Process-Destroyed</td>
<td>EXEC process destroyed.</td>
</tr>
<tr>
<td>29</td>
<td>Close-Virtual-Connection</td>
<td>User closes a virtual connection.</td>
</tr>
<tr>
<td>30</td>
<td>End-Virtual-Connection</td>
<td>Virtual connected has ended.</td>
</tr>
<tr>
<td>31</td>
<td>Exit-Rlogin</td>
<td>User exists Rlogin.</td>
</tr>
<tr>
<td>32</td>
<td>Invalid-Rlogin-Option</td>
<td>Invalid Rlogin option selected.</td>
</tr>
<tr>
<td>33</td>
<td>Insufficient-Resources</td>
<td>Insufficient resources.</td>
</tr>
<tr>
<td>40</td>
<td>Timeout-PPP-LCP</td>
<td>PPP LCP negotiation timed out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Codes 40 through 49 apply to PPP sessions.</td>
</tr>
<tr>
<td>41</td>
<td>Failed-PPP-LCP-Negotiation</td>
<td>PPP LCP negotiation failed.</td>
</tr>
<tr>
<td>42</td>
<td>Failed-PPP-PAP-Auth-Fail</td>
<td>PPP PAP authentication failed.</td>
</tr>
<tr>
<td>43</td>
<td>Failed-PPP-CHAP-Auth</td>
<td>PPP CHAP authentication failed.</td>
</tr>
<tr>
<td>44</td>
<td>Failed-PPP-Remote-Auth</td>
<td>PPP remote authentication failed.</td>
</tr>
<tr>
<td>Cause Code</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>45</td>
<td>PPP-Remote-Terminate</td>
<td>PPP received a Terminate Request from remote end.</td>
</tr>
<tr>
<td>46</td>
<td>PPP-Closed-Event</td>
<td>Upper layer requested that the session be closed.</td>
</tr>
<tr>
<td>47</td>
<td>NCP-Closed-PPP</td>
<td>PPP session closed because there were no NCPs open.</td>
</tr>
<tr>
<td>48</td>
<td>MP-Error-PPP</td>
<td>PPP session closed because of an MP error.</td>
</tr>
<tr>
<td>49</td>
<td>PPP-Maximum-Channels</td>
<td>PPP session closed because maximum channels were reached.</td>
</tr>
<tr>
<td>50</td>
<td>Tables-Full</td>
<td>Disconnect due to full terminal server tables.</td>
</tr>
<tr>
<td>51</td>
<td>Resources-Full</td>
<td>Disconnect due to full internal resources.</td>
</tr>
<tr>
<td>52</td>
<td>Invalid-IP-Address</td>
<td>IP address is not valid for Telnet host.</td>
</tr>
<tr>
<td>53</td>
<td>Bad-Hostname</td>
<td>Hostname cannot be validated.</td>
</tr>
<tr>
<td>54</td>
<td>Bad-Port</td>
<td>Port number is invalid or missing.</td>
</tr>
<tr>
<td>60</td>
<td>Reset-TCP</td>
<td>TCP connection has been reset.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Codes 60 through 67 apply to Telnet or raw TCP sessions.</td>
</tr>
<tr>
<td>61</td>
<td>TCP-Connection-Refused</td>
<td>TCP connection has been refused by the host.</td>
</tr>
<tr>
<td>62</td>
<td>Timeout-TCP</td>
<td>TCP connection has timed out.</td>
</tr>
<tr>
<td>63</td>
<td>Foreign-Host-Close-TCP</td>
<td>TCP connection has been closed.</td>
</tr>
<tr>
<td>64</td>
<td>TCP-Network-Unreachable</td>
<td>TCP network is unreachable.</td>
</tr>
<tr>
<td>65</td>
<td>TCP-Host-Unreachable</td>
<td>TCP host is unreachable.</td>
</tr>
<tr>
<td>66</td>
<td>TCP-Network-Admin Unreachable</td>
<td>TCP network is unreachable for administrative reasons.</td>
</tr>
<tr>
<td>67</td>
<td>TCP-Port-Unreachable</td>
<td>TCP port in unreachable.</td>
</tr>
<tr>
<td>100</td>
<td>Session-Timeout</td>
<td>Session timed out.</td>
</tr>
<tr>
<td>101</td>
<td>Session-Failed-Security</td>
<td>Session failed for security reasons.</td>
</tr>
<tr>
<td>102</td>
<td>Session-End-Callback</td>
<td>Session terminated due to callback.</td>
</tr>
<tr>
<td>120</td>
<td>Invalid-Protocol</td>
<td>Call refused because the detected protocol is disabled.</td>
</tr>
<tr>
<td>150</td>
<td>RADIUS-Disconnect</td>
<td>Disconnected by RADIUS request.</td>
</tr>
<tr>
<td>151</td>
<td>Local-Admin-Disconnect</td>
<td>Administrative disconnect.</td>
</tr>
<tr>
<td>152</td>
<td>SNMP-Disconnect</td>
<td>Disconnected by SNMP request.</td>
</tr>
<tr>
<td>160</td>
<td>V110-Retries</td>
<td>Allowed V.110 retries have been exceeded.</td>
</tr>
<tr>
<td>170</td>
<td>PPP-Authentication-Timeout</td>
<td>PPP authentication timed out.</td>
</tr>
<tr>
<td>Cause Code</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>180</td>
<td>Local-Hangup</td>
<td>Disconnected by local hangup.</td>
</tr>
<tr>
<td>185</td>
<td>Remote-Hangup</td>
<td>Disconnected by remote end hangup.</td>
</tr>
<tr>
<td>190</td>
<td>T1-Quiesced</td>
<td>Disconnected because T1 line was quiesced.</td>
</tr>
<tr>
<td>195</td>
<td>Call-Duration</td>
<td>Disconnected because the maximum duration of the call was exceeded.</td>
</tr>
<tr>
<td>600</td>
<td>VPN-User-Disconnect</td>
<td>Call disconnected by client (through PPP).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Code is sent if the LNS receives a PPP terminate request from the client.</td>
</tr>
<tr>
<td>601</td>
<td>VPN-Carrier-Loss</td>
<td>Loss of carrier. This can be the result of a physical line going dead.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Code is sent when a client is unable to dial out using a dialer.</td>
</tr>
<tr>
<td>602</td>
<td>VPN-No-Resources</td>
<td>No resources available to handle the call.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Code is sent when the client is unable to allocate memory (running low on memory).</td>
</tr>
<tr>
<td>603</td>
<td>VPN-Bad-Control-Packet</td>
<td>Bad L2TP or L2F control packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This code is sent when an invalid control packet, such as missing mandatory Attribute-Value pairs (AVP), from the peer is received. When using L2TP, the code will be sent after six retransmits; when using L2F, the number of retransmits is user configurable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> VPN-Tunnel-Shut will be sent if there are active sessions in the tunnel.</td>
</tr>
<tr>
<td>604</td>
<td>VPN-Admin-Disconnect</td>
<td>Administrative disconnect. This can be the result of a VPN soft shutdown, which is when a client reaches maximum session limit or exceeds maximum hopcount. Code is sent when a tunnel is brought down by issuing the <code>clear vpdn tunnel</code> command.</td>
</tr>
<tr>
<td>605</td>
<td>VPN-Tunnel-Shut</td>
<td>Tunnel teardown or tunnel setup has failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Code is sent when there are active sessions in a tunnel and the tunnel goes down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This code is not sent when tunnel authentication fails.</td>
</tr>
<tr>
<td>606</td>
<td>VPN-Local-Disconnect</td>
<td>Call is disconnected by LNS PPP module.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Code is sent when the LNS sends a PPP terminate request to the client. It indicates a normal PPP disconnection initiated by the LNS.</td>
</tr>
<tr>
<td>607</td>
<td>VPN-Session-Limit</td>
<td>VPN soft shutdown is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Code is sent when a call has been refused due to any of the soft shutdown restrictions previously mentioned.</td>
</tr>
<tr>
<td>608</td>
<td>VPN-Call-Redirect</td>
<td>VPN call redirect is enabled.</td>
</tr>
</tbody>
</table>
RADIUS Progress Codes

The RADIUS Progress Codes feature adds additional progress codes to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.

Attribute 196 is sent in network, exec, and resource accounting “start” and “stop” records. This attribute can facilitate call failure debugging because each progress code identifies accounting information relevant to the connection state of a call. The attribute is activated by default; when an accounting “start” or “stop” accounting record is requested, authentication, authorization, and accounting (AAA) adds attribute 196 into the record as part of the standard attribute list. Attribute 196 is valuable because the progress codes, which are sent in accounting “start” and “stop” records, facilitate the debugging of call failures.

In accounting “start” records, attribute 196 does not have a value.

Table 67: Newly Supported Progress Codes for Attribute 196

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Modem allocation and negotiation is complete; the call is up.</td>
</tr>
<tr>
<td>30</td>
<td>The modem is up.</td>
</tr>
<tr>
<td>33</td>
<td>The modem is waiting for result codes.</td>
</tr>
<tr>
<td>41</td>
<td>The max TNT is establishing the TCP connection by setting up a TCP clear call.</td>
</tr>
<tr>
<td>60</td>
<td>Link control protocol (LCP) is the open state with PPP and IP Control Protocol (IPCP) negotiation; the LAN session is up.</td>
</tr>
<tr>
<td>65</td>
<td>PPP negotiation occurs and, initially, the LCP negotiation occurs; LCP is in the open state.</td>
</tr>
<tr>
<td>67</td>
<td>After PPP negotiation with LCP in the open state occurs, IPCP negotiation begins.</td>
</tr>
</tbody>
</table>

Progress codes 33, 30, and 67 are generated and seen through debugs on the NAS; all other codes are generated and seen through debugs and the accounting record on the RADIUS server.

Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the switch. You specify the RADIUS host and secret text string by using the `radius server` global configuration commands.
Enhanced Test Command

The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or dialed number identification service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls.

How to Configure RADIUS

Identifying the RADIUS Server Host

To apply these settings globally to all RADIUS servers communicating with the Switch, use the three unique global configuration commands: `radius-server timeout`, `radius-server retransmit`, and `radius-server key`.

You can configure the Switch to use AAA server groups to group existing server hosts for authentication. For more information, see Related Topics below.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the Switch and the key string to be shared by both the server and the Switch. For more information, see the RADIUS server documentation.

Follow these steps to configure per-server RADIUS server communication.

**Before you begin**

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these settings on all RADIUS servers, see Related Topics below.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `radius server name`
4. `address {ipv4 | ipv6} ip address {auth-port port number | acct-port port number}`
5. `key string`
6. `retransmit value`
7. `timeout seconds`
8. `end`
9. `show running-config`
10. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Step 2**

**Example:**

Switch# configure terminal

**Step 3**

**Example:**

Switch(config)# radius server ISE

**Step 4**

**Example:**

Switch(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646

**Step 5**

**Example:**

Switch(config-radius-server)# key cisco123

**Note**

The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the `radius server` command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.

**Step 6**

**Example:**

Switch(config-radius-server)# retransmit 10

**Step 7**

**Example:**

Switch(config-radius-server)# timeout 60

(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the `radius-server retransmit` global configuration command setting.

(Optional) Specifies the time interval that the Switch waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the `radius-server timeout` global configuration command setting.
### Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure settings for all RADIUS servers:

#### SUMMARY STEPS

1. `configure terminal`
2. `radius-server key string`
3. `radius-server retransmit retries`
4. `radius-server timeout seconds`
5. `radius-server deadtime minutes`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>Specifies the shared secret text string used between the switch and all RADIUS servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>radius-server key string</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Verifies your entries.

Verifies your entries.

(Optional) Saves your entries in the configuration file.
### Configuring RADIUS Login Authentication

Follow these steps to configure RADIUS login authentication:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# radius-server key your_server_key</td>
<td>The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</td>
</tr>
<tr>
<td>Switch(config)# key your_server_key</td>
<td>Note</td>
</tr>
<tr>
<td>Step 3 radius-server retransmit retries</td>
<td>Specifies the number of times the switch sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server retransmit 5</td>
<td></td>
</tr>
<tr>
<td>Step 4 radius-server timeout seconds</td>
<td>Specifies the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range 1 to 1000.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server timeout 3</td>
<td></td>
</tr>
<tr>
<td>Step 5 radius-server deadtime minutes</td>
<td>When a RADIUS server is not responding to authentication requests, this command specifies a time to stop the request on that server. This avoids the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server deadtime 0</td>
<td></td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 7 show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Before you begin

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login \{default \| list-name\} method1 [method2...]
5. line \{console \| tty \| vty\} line-number [ending-line-number]
6. login authentication \{default \| list-name\}
7. end
8. show running-config
9. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
 Example:  
 Switch> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
 Example:  
 Switch# configure terminal |
| **Step 3** aaa new-model | Enables AAA.  
 Example:  
 Switch(config)# aaa new-model |
| **Step 4** aaa authentication login \{default \| list-name\} method1 [method2...] | Creates a login authentication method list.  
 Example:  
 Switch(config)# aaa authentication login default local |

* To create a default list that is used when a named list is *not* specified in the `login authentication` command, use the `default` keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.

* For `list-name`, specify a character string to name the list you are creating.
Purpose

• For method1..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Select one of these methods:

• **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the `enable password` global configuration command.

• **group radius**—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server.

• **line**—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the `password password` line configuration command.

• **local**—Use the local username database for authentication. You must enter username information in the database. Use the `username name password` global configuration command.

• **local-case**—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the `username password` global configuration command.

• **none**—Do not use any authentication for login.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> line [console</td>
<td>tty</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# line 1 4</td>
</tr>
<tr>
<td><strong>Step 6</strong> login authentication {default</td>
<td>list-name}</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# login authentication default</td>
</tr>
<tr>
<td></td>
<td>• If you specify default, use the default list created with the <code>aaa authentication login</code> command.</td>
</tr>
<tr>
<td></td>
<td>• For list-name, specify the list created with the <code>aaa authentication login</code> command.</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

---

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
### Defining AAA Server Groups

You use the `server` group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional `auth-port` and `acct-port` keywords.

Follow these steps to define AAA server groups:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `radius server name`
4. `address {ipv4 | ipv6} {ip-address | hostname} auth-port port-number acct-port port-number`
5. `key string`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Switch</strong># <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>radius server name</code></td>
<td>Specifies the name of the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode. The switch also supports RADIUS for IPv6.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# radius server ISE</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> `address {ipv4</td>
<td>ipv6} {ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>key string</code></td>
<td>Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-radius-server)# key cisco123</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>end</code></td>
<td>Exits RADIUS server configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-radius-server)# end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring RADIUS Authorization for User Privileged Access and Network Services

**Note**
Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Follow these steps to configure RADIUS authorization for user privileged access and network services:

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa authorization network radius`
4. `aaa authorization exec radius`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** `configure terminal` | Enters global configuration mode. |
| **Example:**  | |
| `Switch# configure terminal`  | |

| **Step 3** `aaa authorization network radius` | Configures the switch for user RADIUS authorization for all network-related service requests. |
| **Example:**  | |
| `Switch(config)# aaa authorization network radius`  | |

| **Step 4** `aaa authorization exec radius` | Configures the switch for user RADIUS authorization if the user has privileged EXEC access. |
| **Example:**  | The `exec` keyword might return user profile information (such as `autocommand` information). |
| `Switch(config)# aaa authorization exec radius`  | |
### What to do next

You can use the `aaa authorization` global configuration command with the `radius` keyword to set parameters that restrict a user’s network access to privileged EXEC mode.

The `aaa authorization exec radius local` command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

### Starting RADIUS Accounting

Follow these steps to start RADIUS accounting:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa accounting network start-stop radius`
4. `aaa accounting exec start-stop radius`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example: Switch&gt; <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa accounting network start-stop radius</td>
<td>Enables RADIUS accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>aaa accounting network start-stop radius</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa accounting exec start-stop radius</td>
<td>Enables RADIUS accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>aaa accounting exec start-stop radius</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example: Switch# <code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

**What to do next**

To establishing a session with a router if the AAA server is unreachable, use the `aaa accounting system guarantee-first` command. This command guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes.
To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.

### Verifying Attribute 196

No configuration is required to configure RADIUS Progress Codes. To verify attribute 196 in accounting “start” and “stop” records, perform the following steps.

**SUMMARY STEPS**

1. `enable`
2. `debug aaa accounting`
3. `show radius statistics`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>debug aaa accounting</code></td>
<td>Displays information on accountable events as they occur.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# debug aaa accounting</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>show radius statistics</code></td>
<td>Displays the RADIUS statistics for accounting and authentication packets.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# debug aaa authorization</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Switch to Use Vendor-Specific RADIUS Attributes

Follow these steps to configure the switch to use vendor-specific RADIUS attributes:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `radius-server vsa send [accounting | authentication]`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Switch # configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`radius-server vsa send [accounting</td>
<td>authentication]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# radius-server vsa send accounting</code></td>
<td>- (Optional) Use the <code>accounting</code> keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

Follow these steps to configure the switch to use vendor-proprietary RADIUS server communication:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. radius-server host \{hostname | ip-address\} non-standard
4. radius-server key string
5. end
6. show running-config
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> radius-server host {hostname</td>
<td>ip-address} non-standard</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# radius-server host 172.20.30.15 non-standard</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> radius-server key string</td>
<td>Specifies the shared secret text string used between the switch and the vendor-proprietary RADIUS server. The switch and the RADIUS server use this text string to encrypt passwords and exchange responses.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# radius-server key rad124</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
### Configuring a User Profile and Associating it with the RADIUS Record

This section describes how to create a named user profile with CLID or DNIS attribute values and associate it with the RADIUS record.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa user profile profile-name`
4. `aaa attribute {dnis | clid}`
5. `exit`
6. `test aaa group {group-name | radius} username password new-code [profile profile-name]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>aaa user profile</strong> <code>profile-name</code></td>
<td>Creates a user profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa user profile profilename1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><strong>aaa attribute</strong> `{dnis</td>
<td>clid}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exit Global Configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><strong>test aaa group</strong> `{group-name</td>
<td>radius} username password new-code [profile profile-name]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# test aaa group radius secret new-code profile profilename1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <code>profile-name</code> must match the profile-name specified in the <code>aaa user profile</code> command.</td>
</tr>
</tbody>
</table>

**Verifying the Enhanced Test Command Configuration**

To verify the Enhanced Test Command configuration, use the following commands in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device# debug radius</code></td>
<td>Displays information associated with RADIUS.</td>
</tr>
<tr>
<td><code>Device# more system:running-config</code></td>
<td>Displays the contents of the current running configuration file. (Note that the <code>more system:running-config</code> command has replaced the <code>show running-config</code> command.)</td>
</tr>
</tbody>
</table>

**Configuration Examples for RADIUS**

**Examples: Identifying the RADIUS Server Host**

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure `host1` as the RADIUS server and to use the default ports for both authentication and accounting:
Example: Using Two Different RADIUS Group Servers

In this example, the switch is configured to recognize two different RADIUS group servers (group1 and group2). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```plaintext
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

Examples: AAA Server Groups

The following example shows how to create server group radgroup1 with three different RADIUS server members, each using the default authentication port (1645) and accounting port (1646):

```plaintext
aaa group server radius radgroup1
server 172.16.1.1
server 172.17.1.21
server 172.18.1.31
```

The following example shows how to create server group radgroup2 with three RADIUS server members, each with the same IP address but with unique authentication and accounting ports:

```plaintext
aaa group server radius radgroup2
server 172.16.1.1 auth-port 1000 acct-port 1001
server 172.16.1.1 auth-port 2000 acct-port 2001
server 172.16.1.1 auth-port 3000 acct-port 3001
```

Troubleshooting Tips for RADIUS Progress Codes

The following example is a sample debug output from the `debug ppp negotiation` command. This debug output is used to verify that accounting “stop” records have been generated and that attribute 196 (Ascend-Connect-Progress) has a value of 65.

```plaintext
Tue Aug 7 06:21:03 2001
  NAS-IP-Address = 10.0.58.62
  NAS-Port = 20018
  Vendor-Specific = 
  NAS-Port-Type = ISDN
  User-Name = "peer_16a"
  Called-Station-Id = "5213124"
  Calling-Station-Id = "5212175"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
```
Examples: Configuring the Switch to Use Vendor-Specific RADIUS Attributes

For example, this AV pair activates Cisco’s *multiple named ip address pools* feature during IP authorization (during PPP IPCP address assignment):

```cisco-avpair= "ip:addr-pool=first"
```

This example shows how to provide a user logging in from a switch with immediate access to privileged EXEC commands:

```cisco-avpair= "shell:priv-lvl=15"
```

This example shows how to specify an authorized VLAN in the RADIUS server database:

```cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-id(#81)=vlanid"
```

This example shows how to apply an input ACL in ASCII format to an interface for the duration of this connection:

```cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

This example shows how to apply an output ACL in ASCII format to an interface for the duration of this connection:

```cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the switch and the server:

```cisco-avpair= "cisco-remote-secret=rad124"
```

*Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)*
Example: User Profile Associated With the test aaa group Command

The following example shows how to configure the dnis = dnisvalue user profile “prfl1” and associate it with a test aaa group command. In this example, the debug radius command has been enabled and the output follows the configuration.

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

```
Example: User Profile Associated With the test aaa group Command

aaa user profile prfl1
    aaa attribute dnis
    aaa attribute dnis dnisvalue
    no aaa attribute clid
! Attribute not found.
    aaa attribute clid clidvalue
    no aaa attribute clid
exit
!
! Associate the dnis user profile with the test aaa group command.
! test aaa group radius user1 pass new-code profile prfl1
!
!
*Dec 31 16:35:48: RADIUS: Sending packet for Unique id = 0
*Dec 31 16:35:48: RADIUS: Initial Transmit unknown id 8 172.22.71.21:1645, Access-Request, len 68
*Dec 31 16:35:48: RADIUS: code=Access-Request id=08 len=0068
    authenticator=1E CA 13 F2 E2 81 57 4C - 02 EA AF 9D 30 D9 97 90
    T=User-Password[2] L=12 V="*
    T=User-Name[1] L=07 V="test"
    T=Called-Station-Id[30] L=0B V="dnisvalue"
    T=Service-Type[6] L=06 V=Login [1]
    T=NAS-IP-Address[4] L=06 V=10.0.1.81

*Dec 31 16:35:48: RADIUS: Received from id 8 172.22.71.21:1645, Access-Accept, len 38
*Dec 31 16:35:48: RADIUS: code=Access-Accept id=08 len=0038
```

Additional References for RADIUS

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
### Related Topic

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco security commands</td>
<td>• Cisco IOS Security Command Reference: Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
<tr>
<td>IPv6 commands</td>
<td>Cisco IOS IPv6 Command Reference</td>
</tr>
</tbody>
</table>

### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 5176</td>
<td>RADIUS Change of Authorization (CoA) extensions</td>
</tr>
</tbody>
</table>

### Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
## Feature Information for RADIUS

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(1)E</td>
<td>The RADIUS Progress Codes feature adds additional progress codes to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates a connection state before a call is disconnected through progress codes.</td>
</tr>
</tbody>
</table>
| Cisco IOS 15.2(1)E                    | The Enhanced Test Command feature allows a named user profile to be created with calling line ID (CLID) or Dialed Number Identification Service (DNIS) attribute values. The CLID or DNIS attribute values can be associated with the RADIUS record that is sent with the user profile so that the RADIUS server can access CLID or DNIS attribute information for all incoming calls.  
The following commands were introduced or modified: `aaa attribute`, `aaa user profile`, and `test aaa group` |
Configuring Accounting

The AAA Accounting feature allows the services that users are accessing and the amount of network resources that users are consuming to be tracked. When AAA Accounting is enabled, the network access server reports user activity to the TACACS+ or RADIUS security server (depending on which security method is implemented) in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

- Finding Feature Information, on page 581
- Prerequisites for Configuring Accounting, on page 581
- Restrictions for Configuring Accounting, on page 582
- Information About Configuring Accounting, on page 582
- How to Configure Accounting, on page 595
- Configuration Examples for Accounting, on page 604
- Additional References for Configuring Accounting, on page 608
- Feature Information for Configuring Accounting, on page 609

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Accounting

The following tasks must be performed before configuring accounting using named method lists:

- Enable AAA on the network access server by using the `aaa new-model` command in global configuration mode.
- Define the characteristics of the RADIUS or TACACS+ security server if RADIUS or TACACS+ authorization is issued. For more information about configuring the Cisco network access server to
Restrictions for Configuring Accounting

- Accounting information can be sent simultaneously to a maximum of only four AAA servers.
- For Service Selection Gateway (SSG) systems, the `aaa accounting network broadcast` command broadcasts only `start-stop` accounting records. If interim accounting records are configured using the `ssg accounting interval` command, the interim accounting records are sent only to the configured default RADIUS server.

Information About Configuring Accounting

Named Method Lists for Accounting

Similar to authentication and authorization method lists, method lists for accounting define the way accounting is performed and the sequence in which these methods are performed.

Named accounting method lists allow particular security protocol to be designated and used on specific lines or interfaces for accounting services. The only exception is the default method list (which is named “default”). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list is simply a named list describing the accounting methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists allow one or more security protocols to be designated and used for accounting, thus ensuring a backup system for accounting in case the initial method fails. Cisco IOS software uses the first method listed to support accounting; if that method fails to respond, the Cisco IOS software selects the next accounting method listed in the method list. This process continues until there is successful communication with a listed accounting method, or all methods defined are exhausted.

Note

The Cisco IOS software attempts accounting with the next listed accounting method only when there is no response from the previous method. If accounting fails at any point in this cycle--meaning that the security server responds by denying the user access--the accounting process stops and no other accounting methods are attempted.

Accounting method lists are specific to the type of accounting being requested. AAA supports seven different types of accounting:

- **Network** -- Provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.
- **EXEC** -- Provides information about user EXEC terminal sessions of the network access server.
- **Commands** -- Provides information about the EXEC mode commands that a user issues. Command accounting generates accounting records for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
• **Connection** -- Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.

• **System** -- Provides information about system-level events.

• **Resource** -- Provides “start” and “stop” records for calls that have passed user authentication, and provides “stop” records for calls that fail to authenticate.

• **VRRS** -- Provides information about Virtual Router Redundancy Service (VRRS).

---

**Note**

System accounting does not use named accounting lists; only the default list for system accounting can be defined.

---

Once again, when a named method list is created, a particular list of accounting methods for the indicated accounting type are defined.

Accounting method lists must be applied to specific lines or interfaces before any of the defined methods are performed. The only exception is the default method list (which is named “default”). If the `aaa accounting` command for a particular accounting type is issued without specifying a named method list, the default method list is automatically applied to all interfaces or lines except those that have a named method list explicitly defined (A defined method list overrides the default method list). If no default method list is defined, then no accounting takes place.

This section includes the following subsections:

### Method Lists and Server Groups

A server group is a way to group existing LDAP, RADIUS, or TACACS+ server hosts for use in method lists. The figure below shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers. R1 and R2 make up the group of RADIUS servers. T1 and T2 make up the group of TACACS+ servers.

Using server groups, a subset of the configured server hosts can be specified and use them for a particular service. For example, server groups allow R1 and R2 to be defined as separate server groups, and T1 and T2 as separate server groups. This allows either R1 and T1 to be specified in the method list or R2 and T2 in the method list, which provides more flexibility in the way that RADIUS and TACACS+ resources are assigned.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. In other words, this unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authorization—the second host entry configured acts as fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order they are configured.)

### AAA Accounting Methods

The Cisco IOS software supports the following two methods for accounting:
Accounting Record Types

For minimal accounting, use the `stop-only` keyword, which instructs the specified method (RADIUS or TACACS+) to send a stop record accounting notice at the end of the requested user process. For more accounting information, use the `start-stop` keyword to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event. To stop all accounting activities on this line or interface, use the `none` keyword.

AAA Accounting Methods

The Cisco IOS software supports the following two methods for accounting:

- TACACS+ -- The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

- RADIUS -- The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Note

With CSCuc32663, passwords and accounting logs are masked before being sent to the TACACS+ or RADIUS security servers. Use the `aaa accounting commands visible-keys` command to send unmasked information to the TACACS+ or RADIUS security servers.

AAA Accounting Types

Network Accounting

Network accounting provides information for all PPP, SLIP, or ARAP sessions, including packet and byte counts.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through an EXEC session:
The following example shows the information contained in a TACACS+ network accounting record for a PPP user who first started an EXEC session:
The precise format of accounting packets records may vary depending on the security server daemon.

The following example shows the information contained in a RADIUS network accounting record for a PPP user who comes in through autoselect:

Wed Jun 27 04:30:52 2001 172.16.25.15 username1 tty4 4327528 start task_id=28
  addr=10.1.1.1 service=ppp protocol=ip
Wed Jun 27 04:36:49 2001 172.16.25.15 username1 tty4 4327528 update
  addr=10.1.1.1 service=ppp protocol=ip

The following example shows the information contained in a TACACS+ network accounting record for a PPP user who comes in through autoselect:

Wed Jun 27 04:02:19 2001 172.16.25.15 username1 Async5 4327528 start task_id=35
  service=ppp

Note: The precise format of accounting packets records may vary depending on the security server daemon.
EXEC Accounting

EXEC accounting provides information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, the access server IP address, and (for dial-in users) the telephone number the call originated from.

The following example shows the information contained in a RADIUS EXEC accounting record for a dial-in user:

Wed Jun 27 04:26:23 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000006"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

NAS-IP-Address = "172.16.25.15"
NAS-Port = 1
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329483"
Acct-Status-Type = Stop
Acct-Session-Time = 62
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

172.16.25.15 username1 tty3 5622329430/4327528
start task_id=2 service=shell
Wed Jun 27 04:08:55 2001
172.16.25.15 username1 tty3 5622329430/4327528
stop task_id=2 service=shell elapsed_time=1354

The following example shows the information contained in a RADIUS EXEC accounting record for a Telnet user:

NAS-IP-Address = "172.16.25.15"
NAS-Port = 26
User-Name = "username1"
Caller-ID = "10.68.202.158"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Command Accounting

Command accounting provides information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the user who executed it.

The following example shows the information contained in a TACACS+ command accounting record for privilege level 1:

```
Wed Jun 27 03:46:47 2001  172.16.25.15  username1  tty3  5622329430/4327528
stop  task_id=3  service=shell  priv-lvl=1  cmd=show version <cr>
Wed Jun 27 03:47:03 2001  172.16.25.15  username1  tty3  5622329430/4327528
stop  task_id=5  service=shell  priv-lvl=1  cmd=show interfaces Ethernet 0 <cr>
Wed Jun 27 03:47:29 2001  172.16.25.15  username1  tty3  5622329430/4327528
stop  task_id=8  service=shell  priv-lvl=15  cmd=ip address 10.1.1.1 255.255.255.0 <cr>
```

The following example shows the information contained in a TACACS+ command accounting record for privilege level 15:

```
Wed Jun 27 03:47:17 2001  172.16.25.15  username1  tty3  5622329430/4327528
stop  task_id=6  service=shell  priv-lvl=15  cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001  172.16.25.15  username1  tty3  5622329430/4327528
stop  task_id=7  service=shell  priv-lvl=15  cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001  172.16.25.15  username1  tty3  5622329430/4327528
stop  task_id=8  service=shell  priv-lvl=15  cmd=ip address 10.1.1.1 255.255.255.0 <cr>
```
The Cisco implementation of RADIUS does not support command accounting.

Connection Accounting

Connection accounting provides information about all outbound connections made from the network access server such as Telnet, LAT, TN3270, PAD, and rlogin.

The following example shows the information contained in a RADIUS connection accounting record for an outbound Telnet connection:

Wed Jun 27 04:28:00 2001
NAS-IP-Address = “172.16.25.15”
NAS-Port = 2
User-Name = “username1”
Client-Port-DNIS = “4327528”
Caller-ID = “5622329477”
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = “00000008”
Login-Service = Telnet
Login-IP-Host = “10.68.202.158”
Acct-Delay-Time = 0
User-Id = “username1”
NAS-Identifier = “172.16.25.15”

NAS-IP-Address = “172.16.25.15”
NAS-Port = 2
User-Name = “username1”
Client-Port-DNIS = “4327528”
Caller-ID = “5622329477”
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = “00000008”
Login-Service = Telnet
Login-IP-Host = “10.68.202.158”
Acct-Delay-Time = 0
User-Id = “username1”
NAS-Identifier = “172.16.25.15”
Acct-Input-Octets = 10774
Acct-Output-Octets = 112
Acct-Input-Packets = 91
Acct-Output-Packets = 99
Acct-Session-Time = 39

The following example shows the information contained in a TACACS+ connection accounting record for an outbound Telnet connection:

Wed Jun 27 03:47:43 2001 172.16.25.15 username1 tty3 5622329430/4327528
start task_id=10 service=connection protocol=telnet addr=10.68.202.158 cmd=telnet
username1-sun

Wed Jun 27 03:48:38 2001 172.16.25.15 username1 tty3 5622329430/4327528
stop task_id=10 service=connection protocol=telnet addr=10.68.202.158 cmd=telnet
username1-sun bytes_in=4467 bytes_out=96 paks_in=61 paks_out=72 elapsed_time=55
The following example shows the information contained in a RADIUS connection accounting record for an outbound rlogin connection:

```
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:30:09 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound rlogin connection:

```
Wed Jun 27 03:48:46 2001 172.16.25.15 username1 tty3 5622329430/4327528
start task_id=12 service=connection protocol=rlogin addr=10.68.202.158 cmd=rlogin
username1-sun /user username1
```

```
Wed Jun 27 03:51:37 2001 172.16.25.15 username1 tty3 5622329430/4327528
stop task_id=12 service=connection protocol=rlogin addr=10.68.202.158 cmd=rlogin
username1-sun /user username1 bytes_in=659926 bytes_out=138 paks_in=2378 paks_out=1251 elapsed_time=171
```

The following example shows the information contained in a TACACS+ connection accounting record for an outbound LAT connection:

```
Wed Jun 27 03:53:06 2001 172.16.25.15 username1 tty3 5622329430/4327528
start task_id=18 service=connection protocol=lat addr=VAX cmd=lat
```

```
Wed Jun 27 03:54:15 2001 172.16.25.15 username1 tty3 5622329430/4327528
stop task_id=18 service=connection protocol=lat addr=VAX cmd=lat
VAX bytes_in=0 bytes_out=0 paks_in=0 paks_out=0 elapsed_time=6
```
System Accounting

System accounting provides information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

The following accounting record shows a typical TACACS+ system accounting record server indicating that AAA Accounting has been turned off:

```
service=system event=sys_acct reason=reconfigure
```

Note

The precise format of accounting packets records may vary depending on the TACACS+ daemon.

The following accounting record shows a TACACS+ system accounting record indicating that AAA Accounting has been turned on:

```
Wed Jun 27 03:55:22 2001 172.16.25.15 unknown unknown unknown stop task_id=23
service=system event=sys_acct reason=reconfigure
```

Additional tasks for measuring system resources are covered in the Cisco IOS software configuration guides. For example, IP accounting tasks are described in the Configuring IP Services chapter in the Cisco IOS Application Services Configuration Guide.

Resource Accounting

The Cisco implementation of AAA accounting provides “start” and “stop” record support for calls that have passed user authentication. The additional feature of generating “stop” records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

This section includes the following subsections:

AAA Resource Failure Stop Accounting

Before AAA resource failure stop accounting, there was no method of providing accounting records for calls that failed to reach the user authentication stage of a call setup sequence. Such records are necessary for users employing accounting records to manage and monitor their networks and their wholesale customers.

This functionality generates a “stop” accounting record for any calls that do not reach user authentication; “stop” records are generated from the moment of call setup. All calls that pass user authentication behave as they did before; that is, no additional accounting records are seen.

The figure below illustrates a call setup sequence with normal call flow (no disconnect) and without AAA resource failure stop accounting enabled.

Figure 46: Modem Dial-In Call Setup Sequence With Normal Flow and Without Resource Failure Stop Accounting Enabled
The figure below illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

**Figure 47: Modem Dial-In Call Setup Sequence With Normal Flow and With Resource Failure Stop Accounting Enabled**

The figure below illustrates a call setup sequence with call disconnect occurring before user authentication and with AAA resource failure stop accounting enabled.

**Figure 48: Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and With Resource Failure Stop Accounting Enabled**

The figure below illustrates a call setup sequence with call disconnect occurring before user authentication and without AAA resource failure stop accounting enabled.

**Figure 49: Modem Dial-In Call Setup Sequence With Call Disconnect Occurring Before User Authentication and Without Resource Failure Stop Accounting Enabled**

**AAA Resource Accounting for Start-Stop Records**

AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.

With this feature, a call setup and call disconnect “start-stop” accounting record tracks the progress of the resource connection to the device. A separate user authentication “start-stop” accounting record tracks the
user management progress. These two sets of accounting records are interlinked by using a unique session ID for the call.

The figure below illustrates a call setup sequence with AAA resource start-stop accounting enabled.

![Modem Dial-In Call Setup Sequence With Resource Start-Stop Accounting Enabled](image)

**VRRS Accounting**

Virtual Router Redundancy Service (VRRS) provides a multiclient information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client. The VRRS multiclient service provides a consistent interface with FHRP protocols by abstracting over several FHRPs and providing an idealized view of their state. VRRS manages data updates, allowing interested clients to register in one place and receive updates for named FHRP groups or all registered FHRP groups.

Virtual Router Redundancy Protocol (VRRP) is an FHRP that acts as a server that pushes FHRP status information out to all registered VRRS clients. Clients obtain status on essential information provided by the FHRP, including current and previous redundancy states, active and inactive L3 and L2 addresses, and, in some cases, information about other redundant gateways in the network. Clients can use this information to provide stateless and stateful redundancy information to clients and protocols.

**VRRS Accounting Plug-in**

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state. The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the `vrrp name` command in interface configuration mode.

The VRRS Accounting plug-in provides a configurable AAA method list mechanism that provides updates to a RADIUS server when a VRRS group transitions its state.

The VRRS accounting plug-in is an extension of existing AAA system accounting messages. The VRRS Accounting plug-in provides accounting-on and accounting-off messages and an additional Vendor-Specific Attribute (VSA) that sends the configured VRRS name in RADIUS accounting messages. The VRRS name is configured using the `vrrp name` command in interface configuration mode. The VRRS Accounting plug-in sends an accounting-on message to RADIUS when a VRRS group transitions to the master state, and it sends an accounting-off message when a VRRS group transitions from the master state.

The following RADIUS attributes are included in VRRS accounting messages by default:

- Attribute 4, NAS-IP-Address
- Attribute 26, Cisco VSA Type 1, VRRS Name
- Attribute 40, Acct-Status-Type
- Attribute 41, Acct-Delay-Time
AAA Accounting Enhancements

AAA Broadcast Accounting

AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously. This functionality allows service providers to send accounting information to their own private AAA servers and to the AAA servers of their end customers. It also provides redundant billing information for voice applications.

Broadcasting is allowed among groups of RADIUS or TACACS+ servers, and each server group can define its backup servers for failover independently of other groups.

Thus, service providers and their end customers can use different protocols (RADIUS or TACACS+) for the accounting server. Service providers and their end customers can also specify their backup servers independently. As for voice applications, redundant accounting information can be managed independently through a separate group with its own failover sequence.

AAA Session MIB

The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using Simple Network Management Protocol (SNMP). The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server. AAA session MIB provides the following information:

- Statistics for each AAA function (when used in conjunction with the show radius statistics command)
- Status of servers providing AAA functions
- Identities of external AAA servers
- Real-time information (such as idle times), providing additional criteria for use by SNMP networks for assessing whether or not to terminate an active call

Note

This command is supported only on Cisco AS5300 and Cisco AS5800 universal access server platforms.

The table below shows the SNMP user-end data objects that can be used to monitor and terminate authenticated client connections with the AAA session MIB feature.

Table 68: SNMP End-User Data Objects

<table>
<thead>
<tr>
<th>SessionId</th>
<th>The session identification used by the AAA Accounting protocol (same value as reported by RADIUS attribute 44 (Acct-Session-ID)).</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserId</td>
<td>The user login ID or zero-length string if a login is unavailable.</td>
</tr>
<tr>
<td>IpAddr</td>
<td>The IP address of the session or 0.0.0.0 if an IP address is not applicable or unavailable.</td>
</tr>
</tbody>
</table>
The elapsed time in seconds that the session has been idle.

Disconnected The session termination object used to disconnect the given client.

CallId The entry index corresponding to this accounting session that the Call Tracker record stored.

The table below describes the AAA summary information provided by the AAA session MIB feature using SNMP on a per-system basis.

<table>
<thead>
<tr>
<th><strong>Table 69: SNMP AAA Session Summary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ActiveTableEntries</strong></td>
</tr>
<tr>
<td><strong>ActiveTableHighWaterMark</strong></td>
</tr>
<tr>
<td><strong>TotalSessions</strong></td>
</tr>
<tr>
<td><strong>DisconnectedSessions</strong></td>
</tr>
</tbody>
</table>

**Accounting Attribute-Value Pairs**

The network access server monitors the accounting functions defined in either TACACS+ AV pairs or RADIUS attributes, depending on which security method is implemented.

**How to Configure Accounting**

**Configuring AAA Accounting Using Named Method Lists**

To configure AAA Accounting using named method lists, perform the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} [method1 [method2...]]
4. Do one of the following:
   • line [aux | console | tty | vty] line-number [ending-line-number]
   • interface interface-type interface-number
5. Do one of the following:
   • accounting {arap | commands level | connection | exec} {default | list-name}
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates an accounting method list and enables accounting. The argument <em>list-name</em> is a character string used to name the created list.</td>
</tr>
<tr>
<td>aaa accounting {system</td>
<td>network</td>
</tr>
<tr>
<td>Example: Device(config)# aaa accounting system default start-stop</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters the line configuration mode for the lines to which the accounting method list is applied.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td>Enters the line configuration mode for the lines to which the accounting method list is applied.</td>
</tr>
<tr>
<td>* line [aux</td>
<td>console</td>
</tr>
<tr>
<td>* interface interface-type interface-number</td>
<td>Enters the interface configuration mode for the interfaces to which the accounting method list is applied.</td>
</tr>
<tr>
<td>Example: Device(config)# line aux line1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Applies the accounting method list to a line or set of lines.</td>
</tr>
<tr>
<td>Do one of the following:</td>
<td>Applies the accounting method list to a line or set of lines.</td>
</tr>
<tr>
<td>* accounting {arap</td>
<td>commands level</td>
</tr>
<tr>
<td>* ppp accounting {default</td>
<td>list-name}</td>
</tr>
<tr>
<td>Example: Device(config-line)# accounting arap default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Exits line configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Device(config-line)# end</td>
<td>(Optional) Exits line configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-line)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring RADIUS System Accounting

Perform this task to configure RADIUS system accounting on the global RADIUS server:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `radius-server accounting system host-config`
5. `aaa group server radius server-name`
6. `server-private {host-name | ip-address} key {0 server-key | 7 server-key} server-key`
7. `accounting system host-config`
8. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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**  
*aaa new-model*  
*Example:*  
Device(config)# aaa new-model | Enables AAA network security services. |
| **Step 4**  
*radius-server accounting system host-config*  
*Example:*  
Device(config)# radius-server accounting system host-config | Enables the device to send a system accounting record for the addition and deletion of a RADIUS server. |
| **Step 5**  
*aaa group server radius server-name*  
*Example:*  
Device(config)# aaa group server radius radgroup1 | Adds the RADIUS server and enters server-group configuration mode.  
- The *server-name* argument specifies the RADIUS server group name. |
| **Step 6**  
*server-private {host-name | ip-address} key {0 server-key | 7 server-key} server-key*  
*Example:* | Enters the hostname or IP address of the RADIUS server and hidden server key. |
Suppressing Generation of Accounting Records for Null Username Sessions

When AAA Accounting is activated, the Cisco IOS software issues accounting records for all users on the system, including users whose username string, because of protocol translation, is NULL. An example of this is users who come in on lines where the `aaa authentication login method-list none` command is applied. To prevent accounting records from being generated for sessions that do not have usernames associated with them, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# aaa accounting suppress null-username</code></td>
<td>Prevents accounting records from being generated for users whose username string is NULL.</td>
</tr>
</tbody>
</table>

Generating Interim Accounting Records

To enable periodic interim accounting records to be sent to the accounting server, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# aaa accounting update [newinfo] periodic number</code></td>
<td>Enables periodic interim accounting records to be sent to the accounting server.</td>
</tr>
</tbody>
</table>
When the `aaa accounting update` command is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword `newinfo` is used, interim accounting records are sent to the accounting server every time there is new accounting information to report. An example of this would be when IPCP completes IP address negotiation with the remote peer. The interim accounting record includes the negotiated IP address used by the remote peer.

When used with the keyword `periodic`, interim accounting records are sent periodically as defined by the `number` argument. The interim accounting record contains all of the accounting information recorded for that user up to the time the interim accounting record is sent.

**Caution**

Using the `aaa accounting update periodic` command can cause heavy congestion when many users are logged in to the network.

### Generating Accounting Records for Failed Login or Session

When AAA Accounting is activated, the Cisco IOS software does not generate accounting records for system users who fail login authentication, or who succeed in login authentication but fail PPP negotiation for some reason.

To specify that accounting stop records be generated for users who fail to authenticate at login or during session negotiation, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# aaa accounting send stop-record authentication failure</code></td>
<td>Generates “stop” records for users who fail to authenticate at login or during session negotiation using PPP.</td>
</tr>
<tr>
<td><code>Device(config)# aaa accounting send stop-record always</code></td>
<td>Sends authentication, authorization, and accounting (AAA) stop records regardless of whether a start record was sent earlier.</td>
</tr>
</tbody>
</table>

### Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records

For PPP users who start EXEC terminal sessions, you can specify the NETWORK records to be generated before EXEC-stop records. In cases such as billing customers for specific services, it can be desirable to keep network start and stop records together, essentially “nesting” them within the framework of the EXEC start and stop messages. For example, a user dialing in using PPP can create the following records: EXEC-start, NETWORK-start, EXEC-stop, NETWORK-stop. By nesting the accounting records, NETWORK-stop records follow NETWORK-start messages: EXEC-start, NETWORK-start, NETWORK-stop, EXEC-stop.

To nest accounting records for user sessions, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Device(config)# aaa accounting nested</code></td>
<td>Nests network accounting records.</td>
</tr>
</tbody>
</table>
## Configuring AAA Resource Failure Stop Accounting

To enable resource failure stop accounting, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa accounting resource method-list stop-failure group server-group</td>
<td>Generates a “stop” record for any calls that do not reach user authentication. <strong>Note</strong> Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 581 section must be performed, and SNMP must be enabled on the network access server.</td>
</tr>
</tbody>
</table>

## Configuring AAA Resource Accounting for Start-Stop Records

To enable full resource accounting for start-stop records, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa accounting resource method-list start-stop group server-group</td>
<td>Supports the ability to send a “start” record at each call setup. followed with a corresponding “stop” record at the call disconnect. <strong>Note</strong> Before configuring this feature, the tasks described in the Prerequisites for Configuring Accounting, on page 581 section must be performed, and SNMP must be enabled on the network access server.</td>
</tr>
</tbody>
</table>

## Configuring AAA Broadcast Accounting

To configure AAA broadcast accounting, use the `aaa accounting` command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa accounting {system</td>
<td>network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa accounting {system</td>
<td>network</td>
</tr>
</tbody>
</table>

## Configuring Per-DNIS AAA Broadcast Accounting

To configure AAA broadcast accounting per DNIS, use the `aaa dnis map accounting network` command in global configuration mode:
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`Device(config)# aaa dnis map dnis-number accounting network [start-stop</td>
<td>Allows per-DNIS accounting configuration. This command has precedence over the global <code>aaa accounting</code> command.</td>
</tr>
<tr>
<td></td>
<td>stop-only</td>
</tr>
</tbody>
</table>

### Configuring AAA Session MIB

The following tasks must be performed before configuring the AAA session MIB feature:

- Configure SNMP.
- Configure AAA.
- Define the RADIUS or TACACS+ server characteristics.

**Note**

Overusing SNMP can affect the overall system performance; therefore, normal network management performance must be considered when this feature is used.

To configure AAA session MIB, use the following command in global configuration mode

**SUMMARY STEPS**

1. `Device (config)# aaa session-mib disconnect`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>Device (config)# aaa session-mib disconnect</code></td>
<td>Monitors and terminates authenticated client connections using SNMP.</td>
</tr>
<tr>
<td></td>
<td>To terminate the call, the <code>disconnect</code> keyword must be used.</td>
</tr>
</tbody>
</table>

### Configuring VRSS Accounting

Perform the following task to configure Virtual Router Redundancy Service (VRSS) to send AAA Accounting messages to the AAA server:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa accounting vrss {default | list-name} start-stop method1 [method2...]`
4. `aaa attribute list list-name`
5. `attribute type name value [service service] [protocol protocol] [mandatory] [tag tag-value]`

6. `exit`

7. `vrrs vrrs-group-name`

8. `accounting delay seconds`

9. `accounting method {default | accounting-method-list}`

10. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa accounting vrrs {default</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa accounting vrrs default start-stop</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa attribute list list-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa attribute list list1</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>attribute type name value [service service] [protocol protocol] [mandatory] [tag tag-value]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-attr-list)# attribute type example</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-attr-list)# exit</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>vrrs vrrs-group-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# vrrs vrrs1</td>
</tr>
</tbody>
</table>
Establishing a Session with a Device if the AAA Server is Unreachable

To establish a console or telnet session with a device if the AAA server is unreachable, use the following command in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# no aaa accounting system guarantee-first</td>
<td>The <strong>aaa accounting system guarantee-first</strong> command guarantees system accounting as the first record, which is the default condition.</td>
</tr>
<tr>
<td></td>
<td>In some situations, users may be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than three minutes. To resolve this problem, the <strong>no aaa accounting system guarantee-first</strong> command can be used.</td>
</tr>
</tbody>
</table>

**Note**
Entering the **no aaa accounting system guarantee-first** command is not the only condition by which the console or telnet session can be started. For example, if the privileged EXEC session is being authenticated by TACACS and the TACACS server is not reachable, then the session cannot start.

Monitoring Accounting

No specific **show** command exists for either RADIUS or TACACS+ accounting. To obtain accounting records displaying information about users currently logged in, use the following command in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# show accounting</td>
<td>Allows display of the active accountable events on the network and helps collect information in the event of a data loss on the accounting server.</td>
</tr>
</tbody>
</table>
Troubleshooting Accounting

To troubleshoot accounting information, use the following command in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# debug aaa accounting</td>
<td>Displays information on accountable events as they occur.</td>
</tr>
</tbody>
</table>

Configuration Examples for Accounting

Example Configuring Named Method List

The following example shows how to configure a Cisco AS5200 (enabled for AAA and communication with a RADIUS security server) in order for AAA services to be provided by the RADIUS server. If the RADIUS server fails to respond, then the local database is queried for authentication and authorization information, and accounting services are handled by a TACACS+ server.

```plaintext
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network blue1 group radius local
aaa accounting network red1 start-stop group radius group tacacs+
username root password ALongPassword
tacacs-server host 172.31.255.0
tacacs-server key goaway
radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd
interface group-async 1
  group-range 1 16
  encapsulation ppp
  ppp authentication chap dialins
  ppp authorization blue1
  ppp accounting red1
line 1 16
  autoselect ppp
  autoselect during-login
  login authentication admins
  modem dialin
```

The lines in this sample RADIUS AAA configuration are defined as follows:

- The `aaa new-model` command enables AAA network security services.

- The `aaa authentication login admins local` command defines a method list “admins”, for login authentication.

- The `aaa authentication ppp dialins group radius local` command defines the authentication method list “dialins”, which specifies that first RADIUS authentication and then (if the RADIUS server does not respond) local authentication is used on serial lines using PPP.

- The `aaa authorization network blue1 group radius local` command defines the network authorization method list named “blue1”, which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed.
The **aaa accounting network red1 start-stop group radius group tacacs+** command defines the network accounting method list named red1, which specifies that RADIUS accounting services (in this case, start and stop records for specific events) are used on serial lines using PPP. If the RADIUS server fails to respond, accounting services are handled by a TACACS+ server.

The **username** command defines the username and password to be used for the PPP Password Authentication Protocol (PAP) caller identification.

The **tacacs-server host** command defines the name of the TACACS+ server host.

The **tacacs-server key** command defines the shared secret text string between the network access server and the TACACS+ server host.

The **radius-server host** command defines the name of the RADIUS server host.

The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.

The **interface group-async** command selects and defines an asynchronous interface group.

The **group-range** command defines the member asynchronous interfaces in the interface group.

The **encapsulation ppp** command sets PPP as the encapsulation method used on the specified interfaces.

The **ppp authentication chap dialins** command selects Challenge Handshake Authentication Protocol (CHAP) as the method of PPP authentication and applies the “dialins” method list to the specified interfaces.

The **ppp authorization blue1** command applies the blue1 network authorization method list to the specified interfaces.

The **ppp accounting red1** command applies the red1 network accounting method list to the specified interfaces.

The **line** command switches the configuration mode from global configuration to line configuration and identifies the specific lines being configured.

The **autoselect ppp** command configures the Cisco IOS software to allow a PPP session to start up automatically on these selected lines.

The **autoselect during-login** command is used to display the username and password prompt without pressing the Return key. After the user logs in, the autoselect function (in this case, PPP) begins.

The **login authentication admins** command applies the admins method list for login authentication.

The **modem dialin** command configures modems attached to the selected lines to only accept incoming calls.

The **show accounting** command yields the following output for the preceding configuration:

```
Active Accounted actions on tty1, User username2 Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
    task_id=5 service=ppp protocol=ip address=10.0.0.98
```

The table below describes the fields contained in the preceding output.
### Example Configuring AAA Resource Accounting

The following example shows how to configure the resource failure stop accounting and resource accounting for start-stop records functions:

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default method to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method to use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

### Example Configuring AAA Broadcast Accounting

The following example shows how to turn on broadcast accounting using the global `aaa accounting` command:

```
 aaa group server radius isp
  server 10.0.0.1
  server 10.0.0.2
aaa group server tacacs+ isp_customer
  server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
```
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2

The broadcast keyword causes “start” and “stop” accounting records for network connections to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

**Example Configuring Per-DNIS AAA Broadcast Accounting**

The following example shows how to turn on per DNIS broadcast accounting using the global `aaa dnis map accounting network` command:

```
aaa group server radius isp
  server 10.0.0.1
  server 10.0.0.2
aaa group server tacacs+ isp_customer
  server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

The broadcast keyword causes “start” and “stop” accounting records for network connection calls having DNIS number 7777 to be sent simultaneously to server 10.0.0.1 in the group isp and to server 172.0.0.1 in the group isp_customer. If server 10.0.0.1 is unavailable, failover to server 10.0.0.2 occurs. If server 172.0.0.1 is unavailable, no failover occurs because backup servers are not configured for the group isp_customer.

**Example AAA Session MIB**

The following example shows how to set up the AAA session MIB feature to disconnect authenticated client connections for PPP users:

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

**Example Configuring VRRS Accounting**

The following example shows how to configure VRRS to send AAA Accounting messages to the AAA server:

```
Router# configure terminal
Router(config)# aaa accounting vrrs vrrp-mlist-1 start-stop group radius
Router(config)# aaa attribute list vrrp-1-attr
Router(config-attr-list)# attribute type account-delay 10
Router(config-attr-list)# exit
Router(config)# vrrs vrrp-group-1
Router(config-vrrs)# accounting delay 10
```
Additional References for Configuring Accounting

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Cisco security commands</td>
<td>• Cisco IOS Security Command Reference: Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2903</td>
<td>Generic AAA Architecture</td>
</tr>
<tr>
<td>RFC 2904</td>
<td>AAA Authorization Framework</td>
</tr>
<tr>
<td>RFC 2906</td>
<td>AAA Authorization Requirements</td>
</tr>
<tr>
<td>RFC 2989</td>
<td>Criteria for Evaluating AAA Protocols for Network Access</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
## Feature Information for Configuring Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Table 71: Feature Information for Configuring Accounting

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Broadcast Accounting</td>
<td>Cisco IOS 15.2(1)E</td>
<td>AAA broadcast accounting allows accounting information to be sent to multiple AAA servers at the same time; that is, accounting information can be broadcast to one or more AAA servers simultaneously.</td>
</tr>
<tr>
<td>AAA Resource Accounting for Start-Stop Records</td>
<td>Cisco IOS 15.2(1)E</td>
<td>AAA resource accounting for start-stop records supports the ability to send a “start” record at each call setup, followed by a corresponding “stop” record at the call disconnect. This functionality can be used to manage and monitor wholesale customers from one source of data reporting, such as accounting records.</td>
</tr>
<tr>
<td>AAA Session MIB</td>
<td>Cisco IOS 15.2(1)E</td>
<td>The AAA session MIB feature allows customers to monitor and terminate their authenticated client connections using SNMP. The data of the client is presented so that it correlates directly to the AAA Accounting information reported by either the RADIUS or the TACACS+ server.</td>
</tr>
<tr>
<td>AAA: IPv6 Accounting Delay Enhancements</td>
<td>Cisco IOS 15.2(1)E</td>
<td>VRSS provides a multiclent information abstraction and management service between a First Hop Redundancy Protocol (FHRP) and a registered client.</td>
</tr>
</tbody>
</table>
Configuring Local Authentication and Authorization

• Finding Feature Information, on page 611
• How to Configure Local Authentication and Authorization, on page 611
• Monitoring Local Authentication and Authorization, on page 613
• Additional References, on page 614
• Feature Information for Local Authentication and Authorization, on page 614

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

How to Configure Local Authentication and Authorization

Configuring the Switch for Local Authentication and Authorization

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. The switch then handles authentication and authorization. No accounting is available in this configuration.

Note

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

Follow these steps to configure AAA to operate without a server by setting the switch to implement AAA in local mode:
### SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login default local
5. aaa authorization exec local
6. aaa authorization network local
7. username name [privilege level] {password encryption-type password}
8. end
9. show running-config
10. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa new-model</td>
</tr>
<tr>
<td></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa authentication login default local</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa authentication login default local</td>
</tr>
<tr>
<td></td>
<td>Sets the login authentication to use the local username database. The <code>default</code> keyword applies the local user database authentication to all ports.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>aaa authorization exec local</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa authorization exec local</td>
</tr>
<tr>
<td></td>
<td>Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>aaa authorization network local</td>
</tr>
<tr>
<td>Example:</td>
<td>Configures user AAA authorization for all network-related service requests.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization network local</code></td>
<td>Enters the local database, and establishes a username-based authentication system.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><strong>username name [privilege level] {password encryption-type password}</strong></td>
<td>Repeat this command for each user.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# username your_user_name privilege 1 password 7 secret567</code></td>
<td>• For <em>name</em>, specify the user ID as one word. Spaces and quotation marks are not allowed.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <em>level</em>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.</td>
</tr>
<tr>
<td></td>
<td>• For <em>encryption-type</em>, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows.</td>
</tr>
<tr>
<td></td>
<td>• For <em>password</em>, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the <em>username</em> command.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>end</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>show running-config</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>copy running-config startup-config</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

**Monitoring Local Authentication and Authorization**

To display Local Authentication and Authorization configuration, use the *show running-config* privileged EXEC command.
Additional References

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for Local Authentication and Authorization

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 34

MAC Authentication Bypass

The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco Identity Based Networking Services (IBNS) and Network Admission Control (NAC) strategy using the client MAC address. The MAC Authentication Bypass feature is applicable to the following network environments:

- Network environments in which a supplicant code is not available for a given client platform.
- Network environments in which the end client configuration is not under administrative control, that is, the IEEE 802.1X requests are not supported on these networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring MAC Authentication Bypass

IEEE 802.1x—Port-Based Network Access Control

You should understand the concepts of port-based network access control and have an understanding of how to configure port-based network access control on your Cisco platform.
**RADIUS and ACLs**

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs). For more information, see the documentation for your Cisco platform and the *Securing User Services Configuration Guide Library*.

The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). For more information, see the *User Guide for Secure ACS Appliance 3.2*.

---

**Information About MAC Authentication Bypass**

**Overview of the Cisco IOS Auth Manager**

The capabilities of devices connecting to a given network can be different, thus requiring that the network support different authentication methods and authorization policies. The Cisco IOS Auth Manager handles network authentication requests and enforces authorization policies regardless of authentication method. The Auth Manager maintains operational data for all port-based network connection attempts, authentications, authorizations, and disconnections and, as such, serves as a session manager.

The possible states for Auth Manager sessions are as follows:

- **Idle**—In the idle state, the authentication session has been initialized, but no methods have yet been run. This is an intermediate state.
- **Running**—A method is currently running. This is an intermediate state.
- **Authc Success**—The authentication method has run successfully. This is an intermediate state.
- **Authc Failed**—The authentication method has failed. This is an intermediate state.
- **Authz Success**—All features have been successfully applied for this session. This is a terminal state.
- **Authz Failed**—At least one feature has failed to be applied for this session. This is a terminal state.
- **No methods**—There were no results for this session. This is a terminal state.

**Overview of the Configurable MAB Username and Password**

A MAC Authentication Bypass (MAB) operation involves authentication using RADIUS Access-Request packets with both the username and password attributes. By default, the username and the password values are the same and contain the MAC address. The Configurable MAB Username and Password feature enables you to configure both the username and the password attributes in the following scenarios:

- To enable MAB for an existing large database that uses formatted username attributes, the username format in the client MAC needs to be configured. Use the `mab request format attribute 1` command to configure the username format.

- Some databases do not accept authentication if the username and password values are the same. In such instances, the password needs to be configured to ensure that the password is different from the username. Use the `mab request format attribute 2` command to configure the password.

The Configurable MAB Username and Password feature allows interoperability between the Cisco IOS Authentication Manager and the existing MAC databases and RADIUS servers. The password is a global
password and hence is the same for all MAB authentications and interfaces. This password is also synchronized across all supervisor devices to achieve high availability.

If the password is not provided or configured, the password uses the same value as the username. The table below describes the formatting of the username and the password:

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Username Format (Group Size, Separator)</th>
<th>Username</th>
<th>Password Configured</th>
<th>Password Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>08002b8619de</td>
<td>(1, :)</td>
<td>0:8:0:0:2:b:8:6:1:9:d:e</td>
<td>None</td>
<td>08:00:2b:86:19:de</td>
</tr>
<tr>
<td></td>
<td>(1, -)</td>
<td>0-8-0-0-2-b-8-6-1-9-d-e</td>
<td></td>
<td>08-00-2b-86-19-de</td>
</tr>
<tr>
<td></td>
<td>(1, .)</td>
<td>0.8.0.0.2.b.8.6.1.9.d.e</td>
<td></td>
<td>08.00.2b.86.19.de</td>
</tr>
<tr>
<td>08002b8619de</td>
<td>(1, :)</td>
<td>0:8:0:0:2:b:8:6:1:9:d:e</td>
<td>Password</td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>(1, -)</td>
<td>0-8-0-0-2-b-8-6-1-9-d-e</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(1, .)</td>
<td>0.8.0.0.2.b.8.6.1.9.d.e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08002b8619de</td>
<td>(2, :)</td>
<td>08:00:2b:86:19:de</td>
<td>None</td>
<td>08:00:2b:86:19:de</td>
</tr>
<tr>
<td></td>
<td>(2, -)</td>
<td>08-00-2b-86-19-de</td>
<td></td>
<td>08-00-2b-86-19-de</td>
</tr>
<tr>
<td></td>
<td>(2, .)</td>
<td>08.00.2b.86.19.de</td>
<td></td>
<td>08.00.2b.86.19.de</td>
</tr>
<tr>
<td>08002b8619de</td>
<td>(2, :)</td>
<td>08:00:2b:86:19:de</td>
<td>Password</td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>(2, -)</td>
<td>08-00-2b-86-19-de</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2, .)</td>
<td>08.00.2b.86.19.de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08002b8619de</td>
<td>(4, :)</td>
<td>0800:2b86:19de</td>
<td>None</td>
<td>0800:2b86:19:de</td>
</tr>
<tr>
<td></td>
<td>(4, -)</td>
<td>0800-2b86-19de</td>
<td></td>
<td>0800-2b86-19:de</td>
</tr>
<tr>
<td></td>
<td>(4, .)</td>
<td>0800.2b86.19de</td>
<td></td>
<td>0800.2b86.19.de</td>
</tr>
<tr>
<td>08002b8619de</td>
<td>(4, :)</td>
<td>0800:2b86:19de</td>
<td>Password</td>
<td>Password</td>
</tr>
<tr>
<td></td>
<td>(4, -)</td>
<td>0800-2b86-19de</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(4, .)</td>
<td>0800.2b86.19de</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08002b8619de</td>
<td>(12, &lt;not applicable&gt;)</td>
<td>08002b8619de</td>
<td>None</td>
<td>08002b8619de</td>
</tr>
<tr>
<td>08002b8619de</td>
<td>(12, &lt;not applicable&gt;)</td>
<td>08002b8619de</td>
<td>Password</td>
<td>Password</td>
</tr>
</tbody>
</table>

How to Configure MAC Authentication Bypass

Enabling MAC Authentication Bypass

Perform this task to enable the MAC Authentication Bypass feature on an 802.1X port.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot / port`
4. `mab`
5. `end`
6. `show authentication sessions interface type slot / port details`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface type slot / port</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface Gigabitethernet 1/2/1 and 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>mab</code></td>
<td>Enables MAB.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# mab</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>show authentication sessions interface type slot / port details</code></td>
<td>Displays the interface configuration and the authenticator instances on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show authentication session interface Gigabitethernet 1/2/1 details and 2/1 details</td>
<td></td>
</tr>
</tbody>
</table>
Enabling Reauthentication on a Port

By default, ports are not automatically reauthenticated. You can enable automatic reauthentication and specify how often reauthentication attempts are made.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot / port
4. switchport
5. switchport mode access
6. authentication port-control auto
7. mab [eap]
8. authentication periodic
9. authentication timer reauthenticate {seconds | server}
10. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>interface type slot / port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface Gigabitethernet 1/2/1</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface Gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Places interface in Layer 2 switched mode.</td>
</tr>
<tr>
<td>switchport</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.</td>
</tr>
<tr>
<td>switchport mode access</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport mode access</td>
<td></td>
</tr>
</tbody>
</table>
### Specifying the Security Violation Mode

When there is a security violation on a port, the port can be shut down or traffic can be restricted. By default, the port is shut down. You can configure the period of time for which the port is shut down.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. switchport
5. switchport mode access
6. authentication port-control auto
7. mab [eap]
8. authentication violation {restrict | shutdown}
9. authentication timer reauthenticate {seconds | server}
10. end

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>authentication port-control auto</td>
<td>Configures the authorization state of the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>mab [eap]</td>
<td>Enables MAB.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# mab</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>authentication periodic</td>
<td>Enables reauthentication.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# authentication periodic</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>authentication timer reauthenticate {seconds</td>
<td>server}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# authentication timer reauthenticate 900</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface <em>type</em> slot / port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# interface Gigabitethernet 1/2/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# interface Gigabitethernet 2/1</td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport</td>
<td>Places interface in Layer 2 switched mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# switchport</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport mode access</td>
<td>Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> authentication port-control auto</td>
<td>Configures the authorization state of the port.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> mab [eap]</td>
<td>Enables MAB.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# mab</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> authentication violation {restrict</td>
<td>shutdown}</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config-if)# authentication violation shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> authentication timer restart <em>seconds</em></td>
<td>Configures the period of time, in seconds, after which an attempt is made to authenticate an unauthorized port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Enabling Configurable MAB Username and Password

SUMMARY STEPS

1. enable
2. configure terminal
3. mab request format attribute 1 groupsize \{1 | 2 | 4 | 12\} separator \{- | : | .\} [lowercase | uppercase]
4. mab request format attribute 2 \[0 | 7\] password
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mab request format attribute 1 groupsize {1</td>
<td>2</td>
</tr>
<tr>
<td>Example: Device(config)# mab request format attribute 1 groupsize 2 separator :</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mab request format attribute 2 [0</td>
<td>7] password</td>
</tr>
<tr>
<td>Example: Device(config)# mab request format attribute 2 password1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for MAC Authentication Bypass

Example: MAC Authentication Bypass Configuration

In the following example, the `mab` command has been configured to enable the MAC Authorization Bypass (MAB) feature on the specified interface. The optional `show authentication sessions` command has been enabled to display the interface configuration and the authentication instances on the interface.

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# mab
Device(config-if)# end
Device# show authentication sessions interface GigabitEthernet2/1 details
```

Example: Enabling Configurable MAB Username and Password

The following example shows how to configure the username format and password for MAC Authentication Bypass (MAB). In this example, the username format is configured as a group of 12 hexadecimal digits with no separator and the global password as `password1`.

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 1 groupsize 2 separator :
Device(config)# mab request format attribute 2 password1
Device(config)# end
```

Additional References for MAC Authentication Bypass

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Authentication commands</td>
<td>• Cisco IOS Security Command Reference: Commands A to C&lt;br&gt;• Cisco IOS Security Command Reference: Commands D to L&lt;br&gt;• Cisco IOS Security Command Reference: Commands M to R&lt;br&gt;• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-AUTH-FRAMEWORK-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td>• CISCO-MAC-AUTH-BYPASS-MIB</td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-PAE-MIB</td>
<td></td>
</tr>
<tr>
<td>• IEEE8021-PAE-MIB</td>
<td></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3580</td>
<td>IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for MAC Authentication Bypass

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfh. An account on Cisco.com is not required.
The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco IBNS and NAC strategy using the client MAC address.

The following commands were introduced or modified: `dot1x mac-auth-bypass, show dot1x interface`.

The Configurable MAB Username and Password feature enables you to configure MAC Authentication Bypass (MAB) username format and password to allow interoperability between the Cisco IOS Authentication Manager and existing MAC databases and RADIUS servers.

The following commands were introduced or modified: `mab request format attribute 1, mab request format attribute 2`.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Authentication Bypass (MAB)</td>
<td>Cisco IOS XE 3.2SE</td>
<td>The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco IBNS and NAC strategy using the client MAC address. The following commands were introduced or modified: <code>dot1x mac-auth-bypass, show dot1x interface</code>.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.3SE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE 3.5E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS 15.2(1)E</td>
<td></td>
</tr>
<tr>
<td>Configurable MAB Username and Password</td>
<td>Cisco IOS 15.2(1)E</td>
<td>The Configurable MAB Username and Password feature enables you to configure MAC Authentication Bypass (MAB) username format and password to allow interoperability between the Cisco IOS Authentication Manager and existing MAC databases and RADIUS servers. The following commands were introduced or modified: <code>mab request format attribute 1, mab request format attribute 2</code>.</td>
</tr>
</tbody>
</table>
Feature Information for MAC Authentication Bypass
Password Strength and Management for Common Criteria

The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords.

For local users, the user profile and the password information with the key parameters are stored on the Cisco device, and this profile is used for local authentication of users. The user can be an administrator (terminal access) or a network user (for example, PPP users being authenticated for network access).

For remote users, where the user profile information is stored in a remote server, a third-party authentication, authorization, and accounting (AAA) server may be used for providing AAA services, both for administrative and network access.

• Finding Feature Information, on page 627
• Restrictions for Password Strength and Management for Common Criteria, on page 628
• Information About Password Strength and Management for Common Criteria, on page 628
• How to Configure Password Strength and Management for Common Criteria, on page 630
• Configuration Examples for Password Strength and Management for Common Criteria, on page 633
• Additional References for Password Strength and Management for Common Criteria, on page 633
• Feature Information for Password Strength and Management for Common Criteria, on page 634

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Restrictions for Password Strength and Management for Common Criteria

Only four concurrent users can log on to the system by using vty at any moment.

Information About Password Strength and Management for Common Criteria

Password Composition Policy

The password composition policy allows you to create passwords of any combination of upper and lowercase characters, numbers, and special characters that include “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, and “)”.

Password Length Policy

The administrator has the flexibility to set the password's minimum and maximum length. The recommended minimum password length is 8 characters. The administrator can specify both the minimum (1) and the maximum (64) length for the password.

Password Lifetime Policy

The security administrator can provide a configurable option for a password to have a maximum lifetime. If the lifetime parameter is not configured, the configured password will never expire. The maximum lifetime can be configured by providing the configurable value in years, months, days, hours, minutes, and seconds. The lifetime configuration will survive across reloads as it is a part of the configuration, but every time the system reboots, the password creation time will be updated to the new time. For example, if a password is configured with a lifetime of one month and on the 29th day, the system reboots, then the password will be valid for one month after the system reboots.

Password Expiry Policy

If the user attempts to log on and if the user's password credentials have expired, then the following happens:

1. The user is prompted to set the new password after successfully entering the expired password.
2. When the user enters the new password, the password is validated against the password security policy.
3. If the new password matches the password security policy, then the AAA database is updated, and the user is authenticated with the new password.
4. If the new password does not match the password security policy, then the user is prompted again for the password. From AAA perspective, there is no restriction on the number of retries. The number of retries for password prompt in case of unsuccessful authentication is controlled by the respective terminal access interactive module. For example, for telnet, after three unsuccessful attempts, the session will be terminated.
If the password's lifetime is not configured for a user and the user has already logged on and if the security administrator configures the lifetime for that user, then the lifetime will be set in the database. When the same user is authenticated the next time, the system will check for password expiry. The password expiry is checked only during the authentication phase.

If the user has been already authenticated and logged on to the system and if the password expires, then no action will be taken. The user will be prompted to change the password only during the next authentication for the same user.

**Password Change Policy**

The new password must contain a minimum of 4 character changes from the previous password. A password change can be triggered by the following scenarios:

- The security administrator wants to change the password.
- The user is trying to get authenticated using a profile, and the password for that profile has expired.

When the security administrator changes the password security policy and the existing profile does not meet the password security policy rules, no action will be taken if the user has already logged on to the system. The user will be prompted to change the password only when the user tries to get authenticated using the profile that does not meet the password security restriction.

When the user changes the password, the lifetime parameters set by the security administrator for the old profile will be the lifetime parameters for the new password.

For noninteractive clients such as dot1x, when the password expires, appropriate error messages will be sent to the clients, and the clients must contact the security administrator to renew the password.

**User Reauthentication Policy**

Users are reauthenticated when they change their passwords.

When users change their passwords on expiry, they will be authenticated against the new password. In such cases, the actual authentication happens based on the previous credentials, and the new password is updated in the database.

---

**Note**

Users can change their passwords only when they are logging on and after the expiry of the old password; however, a security administrator can change the user's password at any time.

**Support for Framed (noninteractive) Session**

When a client such as dot1x uses the local database for authentication, the Password Strength and Management for Common Criteria feature will be applicable; however, upon password expiry, clients will not be able to change the password. An appropriate failure message will be sent to such clients, and the user must request the security administrator to change the password.
How to Configure Password Strength and Management for Common Criteria

Configuring the Password Security Policy

Perform this task to create a password security policy and to apply the policy to a specific user profile.

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa common-criteria policy policy-name
5. char-changes number
6. max-length number
7. min-length number
8. numeric-count number
9. special-case number
10. exit
11. username username common-criteria-policy policy-name password password
12. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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**  
**aaa new-model**  
_Example:_  
Device(config)# aaa new-model | Enables AAA globally. |

| **Step 4**  
**aaa common-criteria policy policy-name**  
_Example:_ | Creates the AAA security password policy and enters common criteria configuration policy mode. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config)# aaa common-criteria policy policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>char-changes number</code></td>
<td>(Optional) Specifies the number of changed characters between old and new passwords.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-cc-policy)# char-changes 4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>max-length number</code></td>
<td>(Optional) Specifies the maximum length of the password.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-cc-policy)# max-length 25</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>min-length number</code></td>
<td>(Optional) Specifies the minimum length of the password.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-cc-policy)# min-length 8</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>numeric-count number</code></td>
<td>(Optional) Specifies the number of numeric characters in the password.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-cc-policy)# numeric-count 4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td><code>special-case number</code></td>
<td>(Optional) Specifies the number of special characters in the password.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-cc-policy)# special-case 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>(Optional) Exits common criteria configuration policy mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-cc-policy)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td><code>username username common-criteria-policy policy-name password password</code></td>
<td>(Optional) Applies a specific policy and password to a user profile.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# username user1 common-criteria-policy policy1 password password</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Verifying the Common Criteria Policy

Perform this task to verify all the common criteria security policies.

**SUMMARY STEPS**

1. `enable`
2. `show aaa common-criteria policy name policy-name`
3. `show aaa common-criteria policy all`

**DETAILED STEPS**

**Step 1** `enable`
Enables privileged EXEC mode.

**Example:**
Device> enable

**Step 2** `show aaa common-criteria policy name policy-name`
Displays the password security policy information for a specific policy.

**Example:**
Device# show aaa common-criteria policy name policy1
Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.

**Step 3** `show aaa common-criteria policy all`
Displays password security policy information for all the configured policies.

**Example:**
Device# show aaa common-criteria policy all
Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.

Policy name: policy2
Minimum length: 1
Maximum length: 34
Upper Count: 10
Configuration Examples for Password Strength and Management for Common Criteria

Example: Password Strength and Management for Common Criteria

The following example shows how to create a common criteria security policy and apply the specific policy to a user profile:

Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1
Device(config)# end

Additional References for Password Strength and Management for Common Criteria

The following sections provide references related to the RADIUS Packet of Disconnect feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>
Feature Information for Password Strength and Management for Common Criteria

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
The Password Strength and Management for Common Criteria feature is used to specify password policies and security mechanisms for storing, retrieving, and providing rules to specify user passwords.

The following commands were introduced or modified: `aaa common-criteria policy`, `debug aaa common-criteria`, and `show aaa common-criteria policy`.
AAA-SERVER-MIB Set Operation

The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the “KEY” under the CISCO-AAA-SERVER-MIB, and delete the AAA server configuration.

• Finding Feature Information, on page 637
• Prerequisites for AAA-SERVER-MIB Set Operation, on page 637
• Restrictions for AAA-SERVER-MIB Set Operation, on page 638
• Information About AAA-SERVER-MIB Set Operation, on page 638
• How to Configure AAA-SERVER-MIB Set Operation, on page 638
• Configuration Examples for AAA-SERVER-MIB Set Operation, on page 639
• Additional References for AAA-SERVER-MIB Set Operation, on page 641
• Feature Information for AAA-SERVER-MIB Set Operation, on page 642

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for AAA-SERVER-MIB Set Operation

AAA must have been enabled on the router, that is, the aaa new-model command must have been configured. If this configuration has not been accomplished, the set operation fails.
Restrictions for AAA-SERVER-MIB Set Operation

Currently, the CISCO SNMP set operation is supported only for the RADIUS protocol. Therefore, only RADIUS servers in global configuration mode can be added, modified, or deleted.

Information About AAA-SERVER-MIB Set Operation

CISCO-AAA-SERVER-MIB

The CISCO-AAA-SERVER-MIB provides that statistics reflect both the state of the AAA server operation with the server itself and of AAA communications with external servers. The CISCO-AAA-SERVER-MIB provides the following information:

• Statistics for each AAA operation
• Status of servers that are providing AAA functions
• Identities of external AAA servers

CISCO-AAA-SERVER-MIB Set Operation

Before Cisco IOS Release 12.4(4)T, the CISCO-AAA-SERVER-MIB supported only the “get” operation. Effective with this release, the CISCO-AAA-SERVER-MIB supports the set operation. With the set operation, you can do the following:

• Create or add a new AAA server.
• Modify the KEY under the CISCO-AAA-SERVER-MIB. This “secret key” is used for secure connectivity to the AAA server, which is present with the network access server (NAS) and the AAA server.
• Delete the AAA server configuration.

How to Configure AAA-SERVER-MIB Set Operation

Configuring AAA-SERVER-MIB Set Operations

No special configuration is required for this feature. The Simple Network Management Protocol (SNMP) framework can be used to manage MIBs. See the Additional References section for a reference to configuring SNMP.

Verifying SNMP Values

SNMP values can be verified by performing the following steps.
SUMMARY STEPS

1. enable
2. show running-config | include radius-server host
3. show aaa servers

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays all the RADIUS servers that are configured in the global configuration mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td>include radius-server host</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show running-config</td>
<td>include radius-server host</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays information about the number of requests sent to and received from authentication, authorization, and accounting (AAA) servers.</td>
</tr>
<tr>
<td>show aaa servers</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show aaa servers</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Examples for AAA-SERVER-MIB Set Operation

RADIUS Server Configuration and Server Statistics Example

The following sample output shows the RADIUS server configuration and server statistics before and after the set operation.

**Before the Set Operation**

Device# show running-config | include radius-server host

! The following line is for server 1.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2
! The following line is for server 2.
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096

**Server Statistics**

Device# show aaa servers

RADIUS: id 2, priority 1, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 25s, previous duration 0s
    Dead: total time 0s, count 7
SNMP Get Operation to Check the Configuration and Statistics of the RADIUS Servers

```
aaa-server5:/users/smetri> getmany 10.0.1.42 casConfigTable
casAddress.2.2 = 172.19.192.238
casAddress.2.3 = 172.19.192.238
casAuthenPort.2.2 = 2095
casAuthenPort.2.3 = 1645
casAcctPort.2.2 = 2096
casAcctPort.2.3 = 1646
casKey.2.2 =
casKey.2.3 =
! The following line shows priority for server 1.
casPriority.2.2 = 1
! The following line shows priority for server 2.
casPriority.2.3 = 2
casConfigRowStatus.2.2 = active(1)
casConfigRowStatus.2.3 = active(1)
aaa-server5:/users/smetri>
```

SNMP Set Operation

The key of the existing RADIUS server is being changed. The index “1” is being used. That index acts as a wildcard for addition, deletion, or modification of any entries.

```
Change the key for server 1:=>
aaa-server5:/users/smetri> setany -v2c 10.0.1.42 public casAddress.2.1 -a 172.19.192.238
casAuthenPort.2.1 -i 2095 casAcctPort.2.1 -i 2096 casKey.2.1 -o king
casAddress.2.1 = 172.19.192.238
casAuthenPort.2.1 = 2095
casAcctPort.2.1 = 2096
casKey.2.1 = king
aaa-server5:/users/smetri>
```
After the Set Operation

After the above SNMP set operation, the configurations on the device change. The following output shows the output after the set operation.

Device# show running-config | include radius-server host

radius-server host 172.19.192.238 auth-port 1645 acct-port 1646
! The following line shows a change in the key value to “king.”
radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key king

Device# show aaa servers

RADIUS: id 3, priority 1, host 172.19.192.238, auth-port 1645, acct-port 1646
State: current UP, duration 189s, previous duration 0s
  Dead: total time 0s, count 2
  Authen: request 8, timeouts 8
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 4
  Author: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
  Account: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0

Elapsed time since counters last cleared: 6m

! The following line shows a new server with new statistics.
RADIUS: id 4, priority 2, host 172.19.192.238, auth-port 2095, acct-port 2096
State: current UP, duration 209s, previous duration 0s
  Dead: total time 0s, count 7
  Authen: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
  Author: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction: success 0, failure 0
  Account: request 0, timeouts 0
    Response: unexpected 0, server error 0, incorrect 0, time 0ms

Additional References for AAA-SERVER-MIB Set Operation

The following sections provide references related to the AAA-SERVER-MIB Set Operation feature.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>
Feature Information for AAA-SERVER-MIB Set Operation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Table 74: Feature Information for AAA-SERVER-MIB Set Operation

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA-SERVER-MIB Set Operation</td>
<td>Cisco IOS 15.2(1)E</td>
<td>The AAA-SERVER-MIB Set Operation feature allows the authentication, authorization, and accounting (AAA) server configuration to be extended or expanded by using the CISCO-AAA-SERVER-MIB to create and add new AAA servers, modify the “KEY” under the CISCO-AAA-SERVER-MIB, and delete the AAA server configuration. The following commands were introduced or modified: <code>show aaa servers</code>, <code>show running-config</code>, <code>show running-config vrf</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 37

Configuring Secure Shell

The Secure Shell (SSH) feature is an application and a protocol that provides a secure replacement to the Berkeley r-tools. The protocol secures sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley reexec and rsh tools. Two versions of SSH are available: SSH Version 1 and SSH Version 2.

- Finding Feature Information, on page 645
- Prerequisites for Configuring Secure Shell, on page 645
- Restrictions for Configuring Secure Shell, on page 646
- Information about SSH, on page 646
- How to Configure Secure Shell, on page 649
- Configuration Examples for Secure Shell, on page 660
- Additional References for Secure Shell, on page 662
- Feature Information for Configuring Secure Shell, on page 662

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the switch for secure shell (SSH):

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.

- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adleman (RSA) key pair.
• SCP relies on SSH for security.
• SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
• A user must have appropriate authorization to use SCP.
• A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the `copy` command. An authorized administrator can also do this from a workstation.
• The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.
• Configure a hostname and host domain for your device by using the `hostname` and `ip domain-name` commands in global configuration mode.

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the Switch for secure shell.

• The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
• SSH supports only the execution-shell application.
• The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
• The Switch supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
• This software release does not support IP Security (IPSec).
• When using SCP, you cannot enter the password into the `copy` command. You must enter the password when prompted.
• The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
• The `-l` keyword and `userid:{number} {ip-address}` delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

Information about SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH and Switch Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).
SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

**SSH Servers, Integrated Clients, and Supported Versions**

The Secure Shell (SSH) Integrated Client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running the SSH server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an unsecured network.

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

---

**Note**

The SSH client functionality is available only when the SSH server is enabled.

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

**RSA Authentication Support**

Rivest, Shamir, and Adleman (RSA) authentication available in Secure Shell (SSH) clients is not supported on the SSH server for Cisco software by default.

**SSL Configuration Guidelines**

When SSL is used in a switch cluster, the SSL session terminates at the cluster commander. Cluster member switches must run standard HTTP.

Before you configure a CA trustpoint, you should ensure that the system clock is set. If the clock is not set, the certificate is rejected due to an incorrect date.

**Secure Copy Protocol Overview**

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.
For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

**Note** When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

### Secure Copy Protocol

Isn’t Secure Copy Protocol related closely enough to SSH that it could be used in this book? I have moved all of the item in this topic to prerequisites or restrictions.

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the switch can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

### How Secure Copy Works

The behavior of Secure Copy (SCP) is similar to that of remote copy (RCP), which comes from the Berkeley r-tools suite (Berkeley university’s own set of networking applications), except that SCP relies on Secure Shell (SSH) for security. In addition, SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so that the device can determine whether the user has the correct privilege level.

SCP allows a user only with a privilege level of 15 to copy any file that exists in the Cisco IOS File System (IFS) to and from a device by using the `copy` command. An authorized administrator may also perform this action from a workstation.

**Note** Enable the SCP option while using the pscp.exe file with the Cisco software.

### Reverse Telnet

Reverse telnet allows you to telnet to a certain port range and connect to terminal or auxiliary lines. Reverse telnet has often been used to connect a Cisco device that has many terminal lines to the consoles of other Cisco devices. Telnet makes it easy to reach the device console from anywhere simply by telnet to the terminal server on a specific line. This telnet approach can be used to configure a device even if all network connectivity to that device is disconnected. Reverse telnet also allows modems that are attached to Cisco devices to be used for dial-out (usually with a rotary device).
Reverse SSH

Reverse telnet can be accomplished using SSH. Unlike reverse telnet, SSH provides for secure connections. The Reverse SSH Enhancements feature provides you with a simplified method of configuring SSH. Using this feature, you no longer have to configure a separate line for every terminal or auxiliary line on which you want to enable SSH. The previous method of configuring reverse SSH limited the number of ports that can be accessed to 100. The Reverse SSH Enhancements feature removes the port number limitation.

How to Configure Secure Shell

Setting Up the Switch to Run SSH

Follow these steps to set up your Switch to run SSH:

**Before you begin**

Configure user authentication for local or remote access. This step is required. For more information, see Related Topics below.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `hostname hostname`
4. `ip domain-name domain_name`
5. `crypto key generate rsa`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>hostname hostname</td>
</tr>
<tr>
<td>Example:</td>
<td>Configures a hostname and IP domain name for your Switch.</td>
</tr>
</tbody>
</table>
### Configuring the SSH Server

Follow these steps to configure the SSH server:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# hostname your_hostname</code></td>
<td><strong>Note</strong> Follow this procedure only if you are configuring the Switch as an SSH server.</td>
</tr>
<tr>
<td><code>Step 4</code> <code>ip domain-name domain_name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Configures a host domain for your Switch.</td>
</tr>
<tr>
<td><code>Switch(config)# ip domain-name your_domain</code></td>
<td></td>
</tr>
<tr>
<td><code>Step 5</code> <code>crypto key generate rsa</code></td>
<td>Enables the SSH server for local and remote authentication on the Switch and generates an RSA key pair. Generating an RSA key pair for the Switch automatically enables SSH.</td>
</tr>
<tr>
<td>Example:</td>
<td>We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.</td>
</tr>
<tr>
<td><code>Switch(config)# crypto key generate rsa</code></td>
<td><strong>Note</strong> Follow this procedure only if you are configuring the Switch as an SSH server.</td>
</tr>
<tr>
<td><code>Step 6</code> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><code>Step 7</code> <code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><code>Step 8</code> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note** This procedure is only required if you are configuring the Switch as an SSH server.
SUMMARY STEPS

1. enable
2. configure terminal
3. ip ssh version [1 | 2]
4. ip ssh {timeout seconds | authentication-retries number}
5. Use one or both of the following:
   • line vt yline_number[ending_line_number]
   • transport input ssh
6. end
7. show running-config
8. copy running-config startup-config

DETAILS STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip ssh version [1</td>
<td>2]</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ip ssh version 1</td>
<td>• 1—Configure the Switch to run SSH Version 1.</td>
</tr>
<tr>
<td></td>
<td>• 2—Configure the Switch to run SSH Version 2.</td>
</tr>
<tr>
<td>If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip ssh {timeout seconds</td>
<td>authentication-retries number}</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ip ssh timeout 90 authentication-retries 2</td>
<td>• Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the Switch uses the default time-out values of the CLI-based sessions.</td>
</tr>
<tr>
<td></td>
<td>By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes.</td>
</tr>
<tr>
<td></td>
<td>• Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.</td>
</tr>
<tr>
<td>Repeat this step when configuring both parameters.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5** Use one or both of the following:

* line vty line_number[ending_line_number]  
* transport input ssh

**Example:**

Switch(config)# line vty 1 10

or

Switch(config-line)# transport input ssh

(Optional) Configures the virtual terminal line settings.

• Enters line configuration mode to configure the virtual terminal line settings. For line_number and ending_line_number, specify a pair of lines. The range is 0 to 15.

• Specifies that the Switch prevent non-SSH Telnet connections. This limits the router to only SSH connections.

**Step 6** end

**Example:**

Switch(config-line)# end

Returns to privileged EXEC mode.

**Step 7** show running-config

**Example:**

Switch# show running-config

Verifies your entries.

**Step 8** copy running-config startup-config

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

---

**Invoking an SSH Client**

Perform this task to invoke the Secure Shell (SSH) client. The SSH client runs in user EXEC mode and has no specific configuration tasks.

**SUMMARY STEPS**

1. enable
2. ssh -l username -vrf vrf-name ip-address
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ssh -l username -vrf vrf-name ip-address</code></td>
<td>Invokes the SSH client to connect to an IP host or address in the specified virtual routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td><code>Device# ssh -l user1 -vrf vrf1 192.0.2.1</code></td>
<td></td>
</tr>
</tbody>
</table>

## Troubleshooting Tips

- If your Secure Shell (SSH) configuration commands are rejected as illegal commands, you have not successfully generated an Rivest, Shamir, and Adleman (RSA) key pair for your device. Make sure that you have specified a hostname and domain. Then use the `crypto key generate rsa` command to generate an RSA key pair and enable the SSH server.

- When configuring the RSA key pair, you might encounter the following error messages:
  - No hostname specified.
    You must configure a hostname for the device using the `hostname` global configuration command.
  - No domain specified.
    You must configure a host domain for the device using the `ip domain-name` global configuration command.

- The number of allowable SSH connections is limited to the maximum number of vtys configured for the device. Each SSH connection uses a vty resource.

- SSH uses either local security or the security protocol that is configured through AAA on your device for user authentication. When configuring Authentication, Authorization, and Accounting (AAA), you must ensure that AAA is disabled on the console for user authentication. AAA authorization is disabled on the console by default. If AAA authorization is enabled on the console, disable it by configuring the `no aaa authorization console` command during the AAA configuration stage.

## Configuring Reverse SSH for Console Access

To configure reverse SSH console access on the SSH server, perform the following steps.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `line line-number ending-line-number`
4. `no exec`
5. `login authentication listname`
6. `transport input ssh`
7. `exit`
8. `exit`
9. `ssh -l userid : {number} {ip-address}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> line line-number ending-line-number</td>
<td>Identifies a line for configuration and enters line configuration mode.</td>
</tr>
<tr>
<td>Example: Device# line 1 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no exec</td>
<td>Disables EXEC processing on a line.</td>
</tr>
<tr>
<td>Example: Device(config-line)# no exec</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> login authentication listname</td>
<td>Defines a login authentication mechanism for the lines.</td>
</tr>
<tr>
<td>Example: Device(config-line)# login authentication default</td>
<td>Note: The authentication method must use a username and password.</td>
</tr>
<tr>
<td><strong>Step 6</strong> transport input ssh</td>
<td>Defines which protocols to use to connect to a specific line of the device.</td>
</tr>
<tr>
<td>Example: Device(config-line)# transport input ssh</td>
<td>• The ssh keyword must be used for the Reverse SSH Enhancements feature.</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits line configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-line)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
Device(config)# exit | Specifies the user ID to use when logging in on the remote networking device that is running the SSH server.

**Step 9**

```plaintext
ssh -l userid : {number} {ip-address}
```

**Example:**

```plaintext
Device# ssh -l lab:1 router.example.com
```

- **userid** -- User ID.
- **: --** Signifies that a port number and terminal IP address will follow the userid argument.
- **number** -- Terminal or auxiliary line number.
- **ip-address** -- Terminal server IP address.

**Note**
The `userid` argument and `:rotary {number} {ip-address}` delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for modem access.

---

### Configuring Reverse SSH for Modem Access

To configure Reverse SSH for modem access, perform the steps shown in the “SUMMARY STEPS” section below.

In this configuration, reverse SSH is being configured on a modem used for dial-out lines. To get any of the dial-out modems, you can use any SSH client and start a SSH session as shown (in Step 10) to get to the next available modem from the rotary device.

### SUMMARY STEPS

1. enable
2. configure terminal
3. line line-number ending-line-number
4. no exec
5. login authentication listname
6. rotary group
7. transport input ssh
8. exit
9. exit
10. ssh -l userid :rotary {number} {ip-address}

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| | • Enter your password if prompted.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Identifies a line for configuration and enters line configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>line line-number ending-line-number</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# line 1 200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>no exec</td>
<td>Enables EXEC processing on a line.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# no exec</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>login authentication listname</td>
<td>Defines a login authentication mechanism for the lines.</td>
</tr>
<tr>
<td><strong>Note</strong> The authentication method must use a username and password.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# login authentication default</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>rotary group</td>
<td>Defines a group of lines consisting of one or more virtual terminal lines or one auxiliary port line.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# rotary 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>transport input ssh</td>
<td>Defines which protocols to use to connect to a specific line of the device.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# transport input ssh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits line configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>ssh -l userid :rotary {number} {ip-address}</td>
<td>Specifies the user ID to use when logging in on the remote networking device that is running the SSH server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# ssh -l lab:rotary1 router.example.com</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting Reverse SSH on the Client

To troubleshoot the reverse SSH configuration on the client (remote device), perform the following steps.

**SUMMARY STEPS**

1. enable
2. debug ip ssh client

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> debug ip ssh client</td>
<td>Displays debugging messages for the SSH client.</td>
</tr>
<tr>
<td>Example: Device# debug ip ssh client</td>
<td></td>
</tr>
</tbody>
</table>

Troubleshooting Reverse SSH on the Server

To troubleshoot the reverse SSH configuration on the terminal server, perform the following steps. The steps may be configured in any order or independent of one another.

**SUMMARY STEPS**

1. enable
2. debug ip ssh
3. show ssh
4. show line
### Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
<td>Shows the version and configuration information for the SSH server.</td>
</tr>
<tr>
<td>show ssh</td>
<td>Shows the status of the SSH server.</td>
</tr>
</tbody>
</table>

### Configuring Secure Copy

To configure a Cisco device for Secure Copy (SCP) server-side functionality, perform the following steps.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `aaa authentication login {default | list-name} method1 [ method2... ]`
5. `aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [ method2... ]]`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2**        |         |
| configure terminal| Enters global configuration mode. |
| Example:          |         |
| Device# configure terminal | |

| **Step 3**        |         |
| aaa new-model     | Sets AAA authentication at login. |
| Example:          |         |
| Device(config)# aaa new-model | |

| **Step 4**        | Enables the AAA access control system. |
| aaa authentication login {default | list-name} method1 [ method2... ] | |
| Example:          |         |
| Device(config)# aaa authentication login default group tacacs+ | |

| **Step 5**        | Sets parameters that restrict user access to a network. |
| aaa authorization {network | exec | commands level | reverse-access | configuration} {default | list-name} [method1 [ method2... ]] | |
| Example:          |         |
| Device(config)# aaa authorization exec default group tacacs+ | |

| **Step 6**        | Establishes a username-based authentication system. |
| username name [privilege level] password encryption-type encrypted-password | |
| Example:          |         |
| Device(config)# username superuser privilege 2 password 0 superpassword | |

| **Step 7**        | Enables SCP server-side functionality. |
| ip scp server enable | |
| Example:          |         |
### Configuration Examples for Secure Shell

#### Example: Secure Copy Configuration Using Local Authentication

The following example shows how to configure the server-side functionality of Secure Copy (SCP). This example uses a locally defined username and password.

```
! AAA authentication and authorization must be configured properly in order for SCP to work.
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
ip scp server enable
```

#### Example: SCP Server-Side Configuration Using Network-Based Authentication

The following example shows how to configure the server-side functionality of SCP using a network-based authentication mechanism:

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```
Example Reverse SSH Console Access

The following configuration example shows that reverse SSH has been configured for console access for terminal lines 1 through 3:

Terminal Server Configuration

```bash
line 1 3
  no exec
  login authentication default
  transport input ssh
```

Client Configuration

The following commands configured on the SSH client will form the reverse SSH session with lines 1, 2, and 3, respectively:

```bash
ssh -l lab:1 router.example.com
ssh -l lab:2 router.example.com
ssh -l lab:3 router.example.com
```

Example Reverse SSH Modem Access

The following configuration example shows that dial-out lines 1 through 200 have been grouped under rotary group 1 for modem access:

```bash
line 1 200
  no exec
  login authentication default
  rotary 1
  transport input ssh
  exit
```

The following command shows that reverse SSH will connect to the first free line in the rotary group:

```bash
ssh -l lab:rotary1 router.example.com
```

Example: Monitoring the SSH Configuration and Status

To verify that the Secure Shell (SSH) server is enabled and to display the version and configuration data for your SSH connection, use the `show ip ssh` command. The following example shows that SSH is enabled:

```bash
Device# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following example shows that SSH is disabled:

```bash
Device# show ip ssh
%SSH has not been enabled
```
To verify the status of your SSH server connections, use the `show ssh` command. The following example shows the SSH server connections on the device when SSH is enabled:

```
Device# show ssh
Connection   Version   Encryption   State   Username
             0 1.5        3DES        Started  guest
```

The following example shows that SSH is disabled:

```
Device# show ssh
%No SSH server connections running.
```

### Additional References for Secure Shell

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Command List, All Releases</em></td>
</tr>
</tbody>
</table>

**Technical Assistance**

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

### Feature Information for Configuring Secure Shell

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td></td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
The **Reverse SSH Enhancements** feature, which is supported for SSH Version 1 and 2, provides an alternative way to configure reverse Secure Shell (SSH) so that separate lines do not need to be configured for every terminal or auxiliary line on which SSH must be enabled. This feature also eliminates the rotary-group limitation.

This feature was supported on CAT4500-X, CAT4500E-SUP6E, CAT4500E-SUP6L-E, CAT4500E-SUP7E, CAT4500E-SUP7L-E.

The following command was introduced: `ssh`.

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.2(1)E</td>
<td>The Reverse SSH Enhancements feature, which is supported for SSH Version 1 and 2, provides an alternative way to configure reverse Secure Shell (SSH) so that separate lines do not need to be configured for every terminal or auxiliary line on which SSH must be enabled. This feature also eliminates the rotary-group limitation. This feature was supported on CAT4500-X, CAT4500E-SUP6E, CAT4500E-SUP6L-E, CAT4500E-SUP7E, CAT4500E-SUP7L-E. The following command was introduced: <code>ssh</code>.</td>
</tr>
</tbody>
</table>
Secure Shell Version 2 Support

The Secure Shell Version 2 Support feature allows you to configure Secure Shell (SSH) Version 2. (SSH Version 1 support was implemented in an earlier Cisco software release.) SSH runs on top of a reliable transport layer and provides strong authentication and encryption capabilities. The only reliable transport that is defined for SSH is TCP. SSH provides a means to securely access and securely execute commands on another computer over a network. The Secure Copy Protocol (SCP) feature that is provided with SSH allows for the secure transfer of files.

- Finding Feature Information, on page 665
- Information About Secure Shell Version 2 Support, on page 665
- How to Configure Secure Shell Version 2 Support, on page 669
- Configuration Examples for Secure Shell Version 2 Support, on page 683
- Additional References for Secure Shell Version 2 Support, on page 688
- Feature Information for Secure Shell Version 2 Support, on page 689

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Secure Shell Version 2 Support

Secure Shell Version 2


The configuration for the SSH Version 2 server is similar to the configuration for SSH Version 1. The `ip ssh version` command defines the SSH version to be configured. If you do not configure this command, SSH by default runs in compatibility mode; that is, both SSH Version 1 and SSH Version 2 connections are honored.
Note

SSH Version 1 is a protocol that has never been defined in a standard. If you do not want your device to fall back to the undefined protocol (Version 1), you should use the `ip ssh version` command and specify Version 2.

The `ip ssh rsa keypair-name` command enables an SSH connection using the Rivest, Shamir, and Adleman (RSA) keys that you have configured. Previously, SSH was linked to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). This behavior still exists, but by using the `ip ssh rsa keypair-name` command, you can overcome this behavior. If you configure the `ip ssh rsa keypair-name` command with a key pair name, SSH is enabled if the key pair exists or SSH will be enabled if the key pair is generated later. If you use this command to enable SSH, you are not forced to configure a hostname and a domain name, which was required in SSH Version 1 of the Cisco software.

Note

The login banner is supported in SSH Version 2, but it is not supported in Secure Shell Version 1.

Secure Shell Version 2 Enhancements

The SSH Version 2 Enhancements feature includes a number of additional capabilities such as supporting Virtual Routing and Forwarding (VRF)-Aware SSH, SSH debug enhancements, and Diffie-Hellman (DH) group exchange support.

Note

The VRF-Aware SSH feature is supported depending on your release.

The Cisco SSH implementation has traditionally used 768-bit modulus, but with an increasing need for higher key sizes to accommodate DH Group 14 (2048 bits) and Group 16 (4096 bits) cryptographic applications, a message exchange between the client and the server to establish the favored DH group becomes necessary. The `ip ssh dh min size` command configures the modulus size on the SSH server. In addition to this, the `ssh` command was extended to add VRF awareness to the SSH client-side functionality through which the VRF instance name in the client is provided with the IP address to look up the correct routing table and establish a connection.

Debugging was enhanced by modifying SSH debug commands. The `debug ip ssh` command was extended to simplify the debugging process. Before the simplification of the debugging process, this command printed all debug messages related to SSH regardless of what was specifically required. The behavior still exists, but if you configure the `debug ip ssh` command with a keyword, messages are limited to information specified by the keyword.

Secure Shell Version 2 Enhancements for RSA Keys

Cisco SSH Version 2 supports keyboard-interactive and password-based authentication methods. The SSH Version 2 Enhancements for RSA Keys feature also supports RSA-based public key authentication for the client and the server.
User authentication—RSA-based user authentication uses a private/public key pair associated with each user for authentication. The user must generate a private/public key pair on the client and configure a public key on the Cisco SSH server to complete the authentication.

An SSH user trying to establish credentials provides an encrypted signature using the private key. The signature and the user’s public key are sent to the SSH server for authentication. The SSH server computes a hash over the public key provided by the user. The hash is used to determine if the server has a matching entry. If a match is found, an RSA-based message verification is performed using the public key. Hence, the user is authenticated or denied access based on the encrypted signature.

Server authentication—While establishing an SSH session, the Cisco SSH client authenticates the SSH server by using the server host keys available during the key exchange phase. SSH server keys are used to identify the SSH server. These keys are created at the time of enabling SSH and must be configured on the client.

For server authentication, the Cisco SSH client must assign a host key for each server. When the client tries to establish an SSH session with a server, the client receives the signature of the server as part of the key exchange message. If the strict host key checking flag is enabled on the client, the client checks if it has the host key entry corresponding to the server. If a match is found, the client tries to validate the signature by using the server host key. If the server is successfully authenticated, the session establishment continues; otherwise, it is terminated and displays a “Server Authentication Failed” message.

---

**Note**

Storing public keys on a server uses memory; therefore, the number of public keys configurable on an SSH server is restricted to ten users, with a maximum of two public keys per user.

**Note**

RSA-based user authentication is supported by the Cisco server, but Cisco clients cannot propose public key as an authentication method. If the Cisco server receives a request from an open SSH client for RSA-based authentication, the server accepts the authentication request.

**Note**

For server authentication, configure the RSA public key of the server manually and configure the `ip ssh stricthostkeycheck` command on the Cisco SSH client.

---

**SNMP Trap Generation**

Depending on your release, Simple Network Management Protocol (SNMP) traps are generated automatically when an SSH session terminates if the traps have been enabled and SNMP debugging has been enabled. For information about enabling SNMP traps, see the “Configuring SNMP Support” module in the [SNMP Configuration Guide](#).

**Note**

When you configure the `snmp-server host` command, the IP address must be the address of the PC that has the SSH (telnet) client and that has IP connectivity to the SSH server.
You must also enable SNMP debugging using the `debug snmp packet` command to display the traps. The trap information includes information such as the number of bytes sent and the protocol that was used for the SSH session.

The following example shows that an SNMP trap is set. The trap notification is generated automatically when the SSH session terminates. In the example, a.b.c.d is the IP address of the SSH client.

```
snmp-server
snmp-server host a.b.c.d public tty
```

The following is sample output from the `debug snmp packet` command. The output provides SNMP trap information for an SSH session.

```
Switch# debug snmp packet
SNMP packet debugging is on
Device1# ssh -l lab 10.0.0.2
Password:
Switch# exit
[Connection to 10.0.0.2 closed by foreign host]
Device1# *Jul 18 10:18:42.619: SNMP: Queuing packet to 10.0.0.2
*Jul 18 10:18:42.619: SNMP: V1 Trap, ent cisco, addr 10.0.0.1, gentrap 6, spectrap 1
local.9.3.1.1.2.1 = 6
tcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 4
ltcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
ltcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 1056
ltcpConnEntry.2.10.0.0.1.22.10.0.0.2.55246 = 1392
local.9.2.1.1.2.1 = lab
*Jul 18 10:18:42.879: SNMP: Packet sent via UDP to 10.0.0.2
```

**SSH Keyboard Interactive Authentication**

The SSH Keyboard Interactive Authentication feature, also known as Generic Message Authentication for SSH, is a method that can be used to implement different types of authentication mechanisms. Basically, any currently supported authentication method that requires only user input can be performed with this feature. The feature is automatically enabled.

The following methods are supported:

- Password
- SecurID and hardware tokens printing a number or a string in response to a challenge sent by the server
- Pluggable Authentication Module (PAM)
- S/KEY (and other One-Time-Pads)
How to Configure Secure Shell Version 2 Support

Configuring a Device for SSH Version 2 Using a Hostname and Domain Name

SUMMARY STEPS

1. enable
2. configure terminal
3. hostname name
4. ip domain-name name
5. crypto key generate rsa
6. ip ssh [time-out seconds | authentication-retries integer]
7. ip ssh version [1 | 2]
8. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures a hostname for your device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# hostname cisco7200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures a domain name for your device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>cisco7200(config)# ip domain-name example.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enables the SSH server for local and remote authentication.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>cisco7200(config)# crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Configures SSH control variables on your device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Device for SSH Version 2 Using RSA Key Pairs

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip ssh rsa keypair-name keypair-name`
4. `crypto key generate rsa usage-keys label key-label modulus modulus-size`
5. `ip ssh [time-out seconds | authentication-retries integer]`
6. `ip ssh version 2`
7. `exit`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip ssh rsa keypair-name keypair-name</td>
<td>Specifies the RSA key pair to be used for SSH.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: A Cisco device can have many RSA key pairs.</td>
</tr>
<tr>
<td>Device(config)# ip ssh rsa keypair-name sshkeys</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> crypto key generate rsa usage-keys label key-label modulus modulus-size</td>
<td>Enables the SSH server for local and remote authentication on the device.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> ip ssh version [1</td>
<td>2]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>cisco7200(config)# ip ssh version 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits global configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Use <code>no hostname</code> command to return to the default host.</td>
</tr>
<tr>
<td>cisco7200(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Cisco SSH Server to Perform RSA-Based User Authentication

#### SUMMARY STEPS

1. enable
2. configure terminal
3. hostname name
4. ip domain-name name
5. crypto key generate rsa
6. ip ssh pubkey-chain
7. username username
8. key-string
9. key-hash key-type key-name
10. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>hostname name</td>
<td></td>
</tr>
<tr>
<td>ip domain-name name</td>
<td></td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td>ip ssh pubkey-chain</td>
<td></td>
</tr>
<tr>
<td>username username</td>
<td></td>
</tr>
<tr>
<td>key-string</td>
<td></td>
</tr>
<tr>
<td>key-hash key-type key-name</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
</tbody>
</table>

### Command or Action

**Example:**

```bash
Device(config)# crypto key generate rsa usage-keys label sshkeys modulus 768
```

**Purpose**

• For SSH Version 2, the modulus size must be at least 768 bits.

**Note**

To delete the RSA key pair, use the `crypto key zeroize rsa` command. When you delete the RSA key pair, you automatically disable the SSH server.

---

**Step 5** ip ssh [time-out seconds | authentication-retries integer]

**Example:**

```bash
Device(config)# ip ssh time-out 12
```

**Purpose**

Configures SSH control variables on your device.

**Step 6** ip ssh version 2

**Example:**

```bash
Device(config)# ip ssh version 2
```

**Purpose**

Specifies the version of SSH to be run on the device.

**Step 7** exit

**Example:**

```bash
Device(config)# exit
```

**Purpose**

Exits global configuration mode and enters privileged EXEC mode.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>hostname name</td>
<td>Specifies the hostname.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# hostname host1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>ip domain-name name</td>
<td>Defines a default domain name that the Cisco software uses to complete unqualified hostnames.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host1(config)# ip domain-name name1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>crypto key generate rsa</td>
<td>Generates RSA key pairs.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host1(config)# crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>ip ssh pubkey-chain</td>
<td>Configures SSH-RSA keys for user and server authentication on the SSH server and enters public-key configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host1(config)# ip ssh pubkey-chain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The user authentication is successful if the RSA public key stored on the server is verified with the public or the private key pair stored on the client.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>username username</td>
<td>Configures the SSH username and enters public-key user configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host1(conf-ssh-pubkey)# username user1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>key-string</td>
<td>Specifies the RSA public key of the remote peer and enters public-key data configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host1(conf-ssh-pubkey-user)# key-string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note You can obtain the public key value from an open SSH client; that is, from the .ssh/id_rsa.pub file.</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>key-hash key-type key-name</td>
<td>(Optional) Specifies the SSH key type and version.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>host1(conf-ssh-pubkey-data)# key-hash ssh-rsa key1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The key type must be ssh-rsa for the configuration of private public key pairs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• This step is optional only if the key-string command is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• You must configure either the key-string command or the key-hash command.</td>
<td></td>
</tr>
</tbody>
</table>
You can use a hashing software to compute the hash of the public key string, or you can also copy the hash value from another Cisco device. Entering the public key data using the `key-string` command is the preferred way to enter the public key data for the first time.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>You can use a hashing software to compute the hash of the public key string, or you can also copy the hash value from another Cisco device. Entering the public key data using the <code>key-string</code> command is the preferred way to enter the public key data for the first time.</td>
</tr>
</tbody>
</table>

**Step 10**

End

**Example:**

```
host1(config-ssh-pubkey-data)# end
```

Exits public-key data configuration mode and returns to privileged EXEC mode.

- Use `no hostname` command to return to the default host.

---

**Configuring the Cisco IOS SSH Client to Perform RSA-Based Server Authentication**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. hostname name
4. ip domain-name name
5. crypto key generate rsa
6. ip ssh pubkey-chain
7. server server-name
8. key-string
9. exit
10. key-hash key-type key-name
11. end
12. configure terminal
13. ip ssh stricthostkeycheck

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| enable
| Example:
| Device> enable
| Enables privileged EXEC mode.
| - Enter your password if prompted. |
| **Step 2**
| configure terminal
| Example:
| Device# configure terminal
<p>| Enters global configuration mode. |</p>
<table>
<thead>
<tr>
<th>Step 3</th>
<th><strong>hostname</strong> name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# hostname host1</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Specifies the hostname.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th><strong>ip domain-name</strong> name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>host1(config)# ip domain-name name1</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Defines a default domain name that the Cisco software uses to complete unqualified hostnames.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th><strong>crypto key generate rsa</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>host1(config)# crypto key generate rsa</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Generates RSA key pairs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>ip ssh pubkey-chain</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>host1(config)# ip ssh pubkey-chain</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Configures SSH-RSA keys for user and server authentication on the SSH server and enters public-key configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th><strong>server</strong> server-name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>host1(conf-ssh-pubkey)# server server1</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enables the SSH server for public-key authentication on the device and enters public-key server configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th><strong>key-string</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>host1(conf-ssh-pubkey-server)# key-string</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Specifies the RSA public-key of the remote peer and enters public key data configuration mode.</td>
</tr>
</tbody>
</table>

**Note** You can obtain the public key value from an open SSH client; that is, from the .ssh/id_rsa.pub file.

<table>
<thead>
<tr>
<th>Step 9</th>
<th><strong>exit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>host1(conf-ssh-pubkey-data)# exit</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Exits public-key data configuration mode and enters public-key server configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th><strong>key-hash</strong> <strong>key-type</strong> <strong>key-name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>host1(conf-ssh-pubkey-server)# key-hash ssh-rsa key1</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>(Optional) Specifies the SSH key type and version.</td>
</tr>
</tbody>
</table>

- The key type must be ssh-rsa for the configuration of private/public key pairs.
- This step is optional only if the **key-string** command is configured.
- You must configure either the **key-string** command or the **key-hash** command.
Starting an Encrypted Session with a Remote Device

The device with which you want to connect must support a Secure Shell (SSH) server that has an encryption algorithm that is supported in Cisco software. Also, you need not enable your device. SSH can be run in disabled mode.

**SUMMARY STEPS**

1. `ssh [-v {1 | 2}] [-c {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | aes192-cbc | aes256-cbc | 3des | aes192-cbc | aes256-cbc}] [-l user-id] [-l user-id:vrf-name number] ip-address ip-address | -l user-id:rotary number ip-address | -m {hmac-md5-128 | hmac-md5-96 | hmac-sha1-160 | hmac-sha1-96} [-o numberofpasswordprompts n] [-p port-num] {ip-addr | hostname} [command] [-vrf]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
Enabling Secure Copy Protocol on the SSH Server

The following task configures the server-side functionality for SCP. This task shows a typical configuration that allows the device to securely copy files from a remote workstation.

### SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login default local
5. aaa authorization exec default local
6. username name privilege privilege-level password password
7. ip ssh time-out seconds
8. ip ssh authentication-retries integer
9. ip scpserverenable
10. exit
11. debug ip scp

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa new-model</td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa new-model</code></td>
<td>Sets AAA authentication at login to use the local username database for authentication.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>aaa authentication login default local</code></td>
<td>Sets the parameters that restrict user access to a network, runs the authorization to determine if the user ID is allowed to run an EXEC shell, and specifies that the system must use the local database for authorization.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa authentication login default local</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>aaa authorization exec default local</code></td>
<td>Establishes a username-based authentication system, and specifies the username, privilege level, and an unencrypted password.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# aaa authorization exec default local</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>username name privilege privilege-level password password</code></td>
<td>Enables the device to securely copy files from a remote workstation.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# username samplename privilege 15 password password1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>ip ssh time-out seconds</code></td>
<td>Sets the time interval (in seconds) that the device waits for the SSH client to respond.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip ssh time-out 120</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>ip ssh authentication-retries integer</code></td>
<td>Sets the number of authentication attempts after which the interface is reset.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip ssh authentication-retries 3</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>ip scp server enable</code></td>
<td>Enables the device to securely copy files from a remote workstation.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# ip scp server enable</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)# exit</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>debug ip scp</code></td>
<td>(Optional) Provides diagnostic information about SCP authentication problems.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>Device# debug ip scp</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Verifying the Status of the Secure Shell Connection

SUMMARY STEPS

1. enable
2. show ssh
3. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>show ssh</td>
<td>Displays the status of SSH server connections.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# show ssh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits privileged EXEC mode and returns to user EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# exit</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following sample output from the `show ssh` command displays status of various SSH Version 1 and Version 2 connections for Version 1 and Version 2 connections:

```
Connection Version Encryption State Username
0 1.5 3DES Session started lab
```

The following sample output from the `show ssh` command displays status of various SSH Version 1 and Version 2 connections for a Version 2 connection with no Version 1 connection:

```
Connection Version Mode Encryption Hmac State Username
```

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
Verifying the Secure Shell Status

SUMMARY STEPS

1. enable
2. show ip ssh
3. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>show ip ssh</td>
<td>Displays the version and configuration data for SSH.</td>
</tr>
<tr>
<td></td>
<td>Example: show ip ssh</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show ip ssh</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Exits privileged EXEC mode and returns to user EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# exit</td>
<td></td>
</tr>
</tbody>
</table>

Examples

The following sample output from the show ip ssh command displays the version of SSH that is enabled, the authentication timeout values, and the number of authentication retries for Version 1 and Version 2 connections:
Monitoring and Maintaining Secure Shell Version 2

**SUMMARY STEPS**

1. enable
2. debug ip ssh
3. debug snmp packet

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>debug ip ssh</td>
<td>Enables debugging of SSH.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# debug ip ssh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>debug snmp packet</td>
<td>Enables debugging of every SNMP packet sent or received by the device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# debug snmp packet</td>
<td></td>
</tr>
</tbody>
</table>
**Example**

The following sample output from the `debug ip ssh` command shows the connection is an SSH Version 2 connection:

```
Device# debug ip ssh
00:33:55: SSH1: starting SSH control process
00:33:55: SSH1: sent protocol version id SSH-1.99-Cisco-1.25
00:33:55: SSH1: protocol version id is - SSH-2.0-OpenSSH_2.5.2p2
00:33:55: SSH2 1: send: len 280 (includes padlen 4)
00:33:55: SSH2 1: SSH2_MSG_KEXINIT sent
00:33:55: SSH2 1: ssh_receive: 536 bytes received
00:33:55: SSH2 1: input: packet len 632
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: ssh_receive: 96 bytes received
00:33:55: SSH2 1: partial packet 8, need 624, maclen 0
00:33:55: SSH2 1: input: padlen 11
00:33:55: SSH2 1: received packet type 20
00:33:55: SSH2 1: SSH2_MSG_KEXINIT received
00:33:55: SSH2: kex: client->server aes128-cbc hmac-md5 none
00:33:55: SSH2: kex: server->client aes128-cbc hmac-md5 none
00:33:55: SSH2 1: expecting SSH2_MSG_KEXDH_INIT
00:33:55: SSH2 1: ssh_receive: 144 bytes received
00:33:55: SSH2 1: input: packet len 144
00:33:55: SSH2 1: partial packet 8, need 136, maclen 0
00:33:55: SSH2 1: input: padlen 5
00:33:55: SSH2 1: received packet type 30
00:33:55: SSH2 1: SSH2_MSG_KEXDH_INIT received
00:33:55: SSH2 1: signature length 111
00:33:55: SSH2 1: send: len 384 (includes padlen 7)
00:33:55: SSH2 1: received packet type 21
00:33:55: SSH2 1: SSH2_MSG_NEWKEYS received
00:33:55: SSH2 1: ssh_receive: 48 bytes received
00:33:55: SSH2 1: input: packet len 48
00:33:55: SSH2 1: partial packet 8, need 8, maclen 0
00:33:55: SSH2 1: input: padlen 10
00:33:55: SSH2 1: newkeys: mode 1
00:33:55: SSH2 1: newkeys: mode 0
00:33:55: SSH2 1: received packet type 2100:33:55: SSH2 1: SSH2_MSG_NEWKEYS received
00:33:56: SSH2 1: ssh_receive: 48 bytes received
00:33:56: SSH2 1: input: packet len 32
00:33:56: SSH2 1: partial packet 16, need 16, maclen 16
00:33:56: SSH2 1: MAC #3 ok
00:33:56: SSH2 1: input: padlen 10
00:33:56: SSH2 1: received packet type 5
00:33:56: SSH2 1: send: len 32 (includes padlen 10)
00:33:56: SSH2 1: done calc MAC out #3
00:33:56: SSH2 1: ssh_receive: 64 bytes received
00:33:56: SSH2 1: input: packet len 48
00:33:56: SSH2 1: partial packet 16, need 32, maclen 16
00:33:56: SSH2 1: MAC #4 ok
00:33:56: SSH2 1: input: padlen 9
00:33:56: SSH2 1: received packet type 50
```
00:33:56: SSH2 1: send: len 32 (includes padlen 13)
00:34:04: SSH2 1: done calc MAC out #4
00:34:04: SSH2 1: ssh_receive: 160 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #5 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 50
00:34:04: SSH2 1: send: len 16 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #5
00:34:04: SSH2 1: authentication successful for lab
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #6 ok
00:34:04: SSH2 1: input: padlen 6
00:34:04: SSH2 1: received packet type 2
00:34:04: SSH2 1: ssh_receive: 64 bytes received
00:34:04: SSH2 1: input: packet len 48
00:34:04: SSH2 1: partial packet 16, need 32, maclen 16
00:34:04: SSH2 1: MAC #7 ok
00:34:04: SSH2 1: input: padlen 19
00:34:04: SSH2 1: received packet type 90
00:34:04: SSH2 1: channel open request
00:34:04: SSH2 1: send: len 32 (includes padlen 10)
00:34:04: SSH2 1: done calc MAC out #6
00:34:04: SSH2 1: ssh_receive: 192 bytes received
00:34:04: SSH2 1: input: packet len 64
00:34:04: SSH2 1: partial packet 16, need 48, maclen 16
00:34:04: SSH2 1: MAC #8 ok
00:34:04: SSH2 1: input: padlen 13
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: pty-reg request
00:34:04: SSH2 1: setting TTY - requested: height 24, width 80; set: height 24, width 80
00:34:04: SSH2 1: input: packet len 96
00:34:04: SSH2 1: partial packet 16, need 80, maclen 16
00:34:04: SSH2 1: MAC #9 ok
00:34:04: SSH2 1: input: padlen 11
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: x11-reg request
00:34:04: SSH2 1: ssh_receive: 48 bytes received
00:34:04: SSH2 1: input: packet len 32
00:34:04: SSH2 1: partial packet 16, need 16, maclen 16
00:34:04: SSH2 1: MAC #10 ok
00:34:04: SSH2 1: input: padlen 12
00:34:04: SSH2 1: received packet type 98
00:34:04: SSH2 1: send: len 32 (includes padlen 10)
00:34:04: SSH2 1: shell request
00:34:04: SSH2 1: shell message received
00:34:04: SSH2 1: starting shell for vty
00:34:04: SSH2 1: send: len 48 (includes padlen 18)
00:34:04: SSH2 1: done calc MAC out #7
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #11 ok
00:34:07: SSH2 1: input: padlen 17
00:34:07: SSH2 1: received packet type 94
00:34:07: SSH2 1: send: len 32 (includes padlen 17)
00:34:07: SSH2 1: done calc MAC out #8
00:34:07: SSH2 1: ssh_receive: 48 bytes received
00:34:07: SSH2 1: input: packet len 32
00:34:07: SSH2 1: partial packet 16, need 16, maclen 16
00:34:07: SSH2 1: MAC #12 ok
00:34:07: SSH2 1: input: padlen 17
Configuration Examples for Secure Shell Version 2 Support

Example: Configuring Secure Shell Version 2

Device# configure terminal
Device(config)# ip ssh version 2

Example: Starting an Encrypted Session with a Remote Device

Device# ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l shaship 10.76.82.24

Example: Configuring Server-Side SCP

The following example shows how to configure the server-side functionality for SCP. This example also configures AAA authentication and authorization on the device. This example uses a locally defined username and password.
Example: Setting an SNMP Trap

The following example shows that an SNMP trap is set. The trap notification is generated automatically when the SSH session terminates. In the example, a.b.c.d is the IP address of the SSH client.

```
snmp-server
snmp-server host a.b.c.d public tty
```

The following is sample output from the `debug snmp packet` command. The output provides SNMP trap information for an SSH session.

```
Device1# debug snmp packet
SNMP packet debugging is on
Device1# ssh -l lab 10.0.0.2
Password:
Device2# exit
[Connection to 10.0.0.2 closed by foreign host]
Device1#
*Jul 18 10:18:42.619: SNMP: Queuing packet to 10.0.0.2
*Jul 18 10:18:42.619: SNMP: V1 Trap, ent cisco, addr 10.0.0.1, gentrap 6, spectrap 1
local.9.3.1.1.2.1 = 6
tcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 4
tcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
tcpConnEntry.11.10.0.0.1.22.10.0.0.2.55246 = 1056
tcpConnEntry.21.10.0.0.1.22.10.0.0.2.55246 = 1392
local.9.2.1.18.2 = lab
*Jul 18 10:18:42.879: SNMP: Packet sent via UDP to 10.0.0.2
Device1#
```

Examples: SSH Keyboard Interactive Authentication

Example: Enabling Client-Side Debugs

The following example shows that the client-side debugs are turned on, and the maximum number of prompts is six (three for the SSH keyboard interactive authentication method and three for the password authentication method).

```
Password:
Password:
Password:
Password:
```

Example: Setting an SNMP Trap

The following example shows that an SNMP trap is set. The trap notification is generated automatically when the SSH session terminates. In the example, a.b.c.d is the IP address of the SSH client.

```
snmp-server
snmp-server host a.b.c.d public tty
```

The following is sample output from the `debug snmp packet` command. The output provides SNMP trap information for an SSH session.

```
Device1# debug snmp packet
SNMP packet debugging is on
Device1# ssh -l lab 10.0.0.2
Password:
Device2# exit
[Connection to 10.0.0.2 closed by foreign host]
Device1#
*Jul 18 10:18:42.619: SNMP: Queuing packet to 10.0.0.2
*Jul 18 10:18:42.619: SNMP: V1 Trap, ent cisco, addr 10.0.0.1, gentrap 6, spectrap 1
local.9.3.1.1.2.1 = 6
tcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 4
tcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
tcpConnEntry.11.10.0.0.1.22.10.0.0.2.55246 = 1056
tcpConnEntry.21.10.0.0.1.22.10.0.0.2.55246 = 1392
local.9.2.1.18.2 = lab
*Jul 18 10:18:42.879: SNMP: Packet sent via UDP to 10.0.0.2
Device1#
```

Examples: SSH Keyboard Interactive Authentication

Example: Enabling Client-Side Debugs

The following example shows that the client-side debugs are turned on, and the maximum number of prompts is six (three for the SSH keyboard interactive authentication method and three for the password authentication method).

```
Password:
Password:
Password:
Password:
```
Password: cisco123
Last login: Tue Dec 6 13:15:21 2005 from 10.76.248.213
user1@courier:~> exit
logout
[Connection to 10.76.248.200 closed by foreign host]
Device1# debug ip ssh client
SSH Client debugging is on
Device1# ssh -l lab 10.1.1.3
Password:
Password:
Password:
Password:
Password:
Password:
Password:
Device2>

Example: Enabling ChPass with a Blank Password Change

In the following example, the ChPass feature is enabled, and a blank password change is accomplished using the SSH Keyboard Interactive Authentication method. A TACACS+ access control server (ACS) is used as the back-end AAA server.

Device1# ssh -l cisco 10.1.1.3
Password:
Old Password: cisco
New Password: cisco123
Re-enter New password: cisco123
Device2> exit
[Connection to 10.1.1.3 closed by foreign host]

Example: Enabling ChPass and Changing the Password on First Login

In the following example, the ChPass feature is enabled and TACACS+ ACS is used as the back-end server. The password is changed on the first login using the SSH keyboard interactive authentication method.

Device1# ssh -l cisco 10.1.1.3
Password: cisco
Your password has expired.
Enter a new one now.
Example: Enabling ChPass and Expiring the Password After Three Logins

In the following example, the ChPass feature is enabled and TACACS+ ACS is used as the back-end AAA server. The password expires after three logins using the SSH keyboard interactive authentication method.

Device1# ssh -l cisco 10.1.1.3
Password: cisco
Device2> exit
[Connection to 10.1.1.3 closed by foreign host]

Device1# ssh -l cisco 10.1.1.3
Password: cisco
Device2> exit

Device1# ssh -l cisco 10.1.1.3
Password: cisco
Device2> exit

Device1# ssh -l cisco 10.1.1.3
Password: cisco
Your password has expired.
Enter a new one now.
New Password: cisco
Re-enter New password: cisco
Try again.
New Password: cisco
Re-enter New password: cisco
Device2>
Example: SNMP Debugging

The following is sample output from the `debug snmp packet` command. The output provides SNMP trap information for an SSH session.

```
Device1# debug snmp packet
SNMP packet debugging is on
Device1# ssh -l lab 10.0.0.2
Password: 
Device2# exit

[Connection to 10.0.0.2 closed by foreign host]
Device1#
```

Example: SSH Debugging Enhancements

The following is sample output from the `debug ip ssh detail` command. The output provides debugging information about the SSH protocol and channel requests.

```
Device# debug ip ssh detail
00:04:22: SSH0: starting SSH control process
00:04:22: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
00:04:22: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
00:04:22: SSH2 0: SSH2_MSG_KEXINIT sent
00:04:22: SSH2 0: SSH2_MSG_KEXINIT received
00:04:22: SSH2:ke: client->server encaes128-cbc mac:hmac-sha1
00:04:22: SSH2:ke: server->client encaes128-cbc mac:hmac-sha1
00:04:22: SSH2 0: expecting SSH2_MSG_KEXDH_INIT
00:04:22: SSH2 0: SSH2_MSG_KEXDH_INIT received
00:04:22: SSH2: kex_derive_keys complete
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS sent
00:04:22: SSH2 0: waiting for SSH2_MSG_NEWKEYS
00:04:22: SSH2 0: SSH2_MSG_NEWKEYS received
00:04:24: SSH2 0: authentication successful for lab
00:04:24: SSH2 0: channel open request
00:04:24: SSH2 0: pty-req request
00:04:24: SSH2 0: setting TTY - requested: height 24, width 80; set: height 24, width 80
00:04:24: SSH2 0: shell request
00:04:24: SSH2 0: shell message received
00:04:24: SSH2 0: starting shell for vty
00:04:38: SSH0: Session terminated normally
```

The following is sample output from the `debug ip ssh packet` command. The output provides debugging information about the SSH packet.
Device# debug ip ssh packet

00:05:43: SSH2 0: send: packet of length 280 (length also includes padlen of 4)
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 280 bytes
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 272 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: input: total packet length of 144 bytes
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 64 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 136 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 136 bytes, maclen 0
00:05:43: SSH2 0: input: total packet length of 16 bytes
00:05:43: SSH2 0: partial packet length(block size) 8 bytes, needed 8 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 16 bytes received
00:05:43: SSH2 0: ssh_receive: 52 bytes received
00:05:43: SSH2 0: input: total packet length of 32 bytes
00:05:43: SSH2 0: partial packet length(block size) 16 bytes, needed 16 bytes, maclen 20
00:05:43: SSH2 0: MAC compared for #3: ok

Additional References for Secure Shell Version 2 Support

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>Cisco security commands</td>
<td>• Cisco IOS Security Command Reference: Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
</tbody>
</table>
## Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF Secure Shell Version 2 Draft Standards</td>
<td>Internet Engineering Task Force website</td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

## Feature Information for Secure Shell Version 2 Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Table 76: Feature Information for Secure Shell Version 2 Support

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Shell Version 2 Client and Server Support</td>
<td>Cisco IOS XE Release 3.4SG</td>
<td>The Cisco image was updated to provide for the automatic generation of SNMP traps when an SSH session terminates. This feature was supported on CAT2960, CAT3560E, CAT3560X, CAT3750, CAT3750E, CAT3750X, CAT4500.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure Shell Version 2 Enhancements</td>
<td>Cisco IOS XE Release 3.4SG</td>
<td>The Secure Shell Version 2 Enhancements feature includes a number of additional capabilities such as support for VRF-Aware SSH, SSH debug enhancements, and DH Group 14 and Group 16 exchange support. This feature was supported on CAT2960, CAT3560E, CAT3560X, CAT3750, CAT3750E, CAT3750X, CAT4500. Note The VRF-Aware SSH feature is supported depending on your release. The following commands were introduced or modified: <code>debug ip ssh</code>, and <code>ip ssh dh min size</code>.</td>
</tr>
<tr>
<td>Secure Shell Version 2 Enhancements for RSA Keys</td>
<td>Cisco IOS XE Release 3.4SG</td>
<td>The Secure Shell Version 2 Enhancements for RSA Keys feature includes a number of additional capabilities to support RSA key-based user authentication for SSH and SSH server host key storage and verification. This feature was supported on CAT2960, CAT3560E, CAT3560X, CAT3750, CAT3750E, CAT3750X, CAT4500.</td>
</tr>
<tr>
<td>Secure Shell Version 2 Support</td>
<td>Cisco IOS XE Release 3.4SG</td>
<td>The Secure Shell Version 2 Support feature allows you to configure Secure Shell (SSH) Version 2 (SSH Version 1 support was implemented in an earlier Cisco software release). SSH runs on top of a reliable transport layer and provides strong authentication and encryption capabilities. This feature was supported on CAT2960, CAT3560E, CAT3560X, CAT3750, CAT3750E, CAT3750X, CAT4500. The following commands were introduced or modified: <code>debug ip ssh</code>, <code>ip ssh min dh size</code>, <code>ip ssh rsa keypair-name</code>, <code>ip ssh version</code>, and <code>ssh</code>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSH Keyboard Interactive Authentication</td>
<td>Cisco IOS XE Release 3.4SG</td>
<td>The SSH Keyboard Interactive Authentication feature, also known as Generic Message Authentication for SSH, is a method that can be used to implement different types of authentication mechanisms. Basically, any currently supported authentication method that requires only user input can be performed with this feature. This feature was supported on CAT2960, CAT3560E, CAT3560X, CAT3750, CAT3750E, CAT3750X, CAT4500.</td>
</tr>
</tbody>
</table>
CHAPTER 39

X.509v3 Certificates for SSH Authentication

The X.509v3 Certificates for SSH Authentication feature uses public key algorithm (PKI) for server and user authentication, and allows the Secure Shell (SSH) protocol to verify the identity of the owner of a key pair via digital certificates, signed and issued by a Certificate Authority (CA).

This module describes how to configure server and user certificate profiles for a digital certificate.

- Finding Feature Information, on page 693
- Prerequisites for X.509v3 Certificates for SSH Authentication, on page 693
- Restrictions for X.509v3 Certificates for SSH Authentication, on page 694
- Information About X.509v3 Certificates for SSH Authentication, on page 694
- How to Configure X.509v3 Certificates for SSH Authentication, on page 695
- Verifying the Server and User Authentication Using Digital Certificates, on page 698
- Configuration Examples for X.509v3 Certificates for SSH Authentication, on page 699
- Additional References for X.509v3 Certificates for SSH Authentication, on page 699
- Feature Information for X.509v3 Certificates for SSH Authentication, on page 700

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for X.509v3 Certificates for SSH Authentication

The X.509v3 Certificates for SSH Authentication feature replaces the `ip ssh server authenticate user` command with the `ip ssh server algorithm authentication` command. Configure the `default ip ssh server authenticate user` command to remove the `ip ssh server authenticate user` command from the configuration. The IOS secure shell (SSH) server will start using the `ip ssh server algorithm authentication` command.

When you configure the `ip ssh server authenticate user` command, the following message is displayed:
Restrictions for X.509v3 Certificates for SSH Authentication

- The X.509v3 Certificates for SSH Authentication feature implementation is applicable only on the Cisco IOS Secure Shell (SSH) server side.
- The Cisco IOS SSH server supports only the x509v3-ssh-rsa algorithm-based certificate for server and user authentication.

Warning

SSH command accepted; but this CLI will be deprecated soon. Please move to new CLI `ip ssh server algorithm authentication`. Please configure the “default ip ssh server authenticate user” to make the CLI ineffective.

Restrictions for X.509v3 Certificates for SSH Authentication

Information About X.509v3 Certificates for SSH Authentication

X.509v3 Certificates for SSH Authentication Overview

The Secure Shell (SSH) protocol provides a secure remote access connection to network devices. The communication between the client and server is encrypted.

There are two SSH protocols that use public key cryptography for authentication. The Transport Layer Protocol, uses a digital signature algorithm (called the public key algorithm) to authenticate the server to the client. And the User Authentication Protocol uses a digital signature to authenticate (public key authentication) the client to the server.

The validity of the authentication depends upon the strength of the linkage between the public signing key and the identity of the signer. Digital certificates, such as those in X.509 Version 3 (X.509v3), are used to provide identity management. X.509v3 uses a chain of signatures by a trusted root certification authority and intermediate certificate authorities to bind a public signing key to a specific digital identity. This implementation allows the use of a public key algorithm for server and user authentication, and allows SSH to verify the identity of the owner of a key pair via digital certificates, signed and issued by a Certificate Authority (CA).

Server and User Authentication Using X.509v3

For server authentication, the Secure shell (SSH) server sends its own certificate to the SSH client for verification. This server certificate is associated with the trustpoint configured in the server certificate profile (ssh-server-cert-profile-server configuration mode).

For user authentication, the SSH client sends the user's certificate to the IOS SSH server for verification. The SSH server validates the incoming user certificate using public key infrastructure (PKI) trustpoints configured in the server certificate profile (ssh-server-cert-profile-user configuration mode).

By default, certificate-based authentication is enabled for server and user at the IOS SSH server end.
OCSP Response Stapling

The Online Certificate Status Protocol (OCSP) enables applications to determine the (revocation) state of an identified certificate. This protocol specifies the data that needs to be exchanged between an application checking the status of a certificate and the server providing that status. An OCSP client issues a status request to an OCSP responder and suspends acceptance of the certificate until a response is received. An OCSP response at a minimum consists of a responseStatus field that indicates the processing status of the request.

For the public key algorithms, the key format consists of a sequence of one or more X.509v3 certificates followed by a sequence of zero or more OCSP responses.

The X.509v3 Certificate for SSH Authentication feature uses OCSP Response Stapling. By using OCSP response stapling, a device obtains the revocation information of its own certificate by contacting the OCSP server and then stapling the result along with its certificates and sending the information to the peer rather than having the peer contact the OCSP responder.

How to Configure X.509v3 Certificates for SSH Authentication

Configuring Digital Certificates for Server Authentication

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip ssh server algorithm hostkey \{x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]\}
4. ip ssh server certificate profile
5. server
6. trustpoint sign PKI-trustpoint-name
7. ocsp-response include
8. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip ssh server algorithm hostkey {x509v3-ssh-rsa [ssh-rsa]</td>
<td>ssh-rsa [x509v3-ssh-rsa]}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

The IOS SSH server must have at least one configured host key algorithm:

- **x509v3-ssh-rsa**—certificate-based authentication
- **ssh-rsa**—public key-based authentication

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><code>ip ssh server certificate profile</code></td>
<td>Configures server and user certificate profiles and enters SSH certificate profile configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip ssh server certificate profile</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>server</code></td>
<td>Configures server certificate profile and enters SSH server certificate profile server configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(ssh-server-cert-profile)# server</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>trustpoint sign PKI-trustpoint-name</code></td>
<td>Attaches the public key infrastructure (PKI) trustpoint to the server certificate profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(ssh-server-cert-profile-server)# trustpoint sign trust1</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>ocsp-response include</code></td>
<td>(Optional) Sends the Online Certificate Status Protocol (OCSP) response or OCSP stapling along with the server certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(ssh-server-cert-profile-server)# ocsp-response include</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>end</code></td>
<td>Exits SSH server certificate profile server configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(ssh-server-cert-profile-server)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Digital Certificates for User Authentication

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip ssh server algorithm authentication` `publickey | keyboard | password`
4. `ip ssh server algorithm publickey` `x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]`
5. `ip ssh server certificate profile`
6. `user`
7. **trustpoint verify PKI-trustpoint-name**
8. **ocsp-response required**
9. **end**

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted.  |
| **Example:**  
  Switch> enable | |
| **Step 2** configure terminal | Enters global configuration mode.  |
| **Example:**  
  Switch# configure terminal | |
| **Step 3** ip ssh server algorithm authentication {publickey | keyboard | password} | Defines the order of user authentication algorithms. Only the configured algorithm is negotiated with the Secure Shell (SSH) client.  
  - The IOS SSH server must have at least one configured user authentication algorithm.  
  - To use the certificate method for user authentication, the publickey keyword must be configured.  |
| **Example:**  
  Switch(config)# ip ssh server algorithm authentication publickey | |
| **Step 4** ip ssh server algorithm publickey {x509v3-ssh-rsa | ssh-rsa | x509v3-ssh-rsa} | Defines the order of public key algorithms. Only the configured algorithm is accepted by the SSH client for user authentication.  
  - The IOS SSH client must have at least one configured public key algorithm:  
    - **x509v3-ssh-rsa**—Certificate-based authentication  
    - **ssh-rsa**—Public-key-based authentication  |
| **Example:**  
  Switch(config)# ip ssh server algorithm publickey x509v3-ssh-rsa | |
| **Step 5** ip ssh server certificate profile | Configures server certificate profile and user certificate profile and enters SSH certificate profile configuration mode.  |
| **Example:**  
  Switch(config)# ip ssh server certificate profile | |
| **Step 6** user | Configures user certificate profile and enters SSH server certificate profile user configuration mode.  |
| **Example:**  
  Switch(ssh-server-cert-profile)# user | |
| **Step 7** trustpoint verify PKI-trustpoint-name | Configures the public key infrastructure (PKI) trustpoint that is used to verify the incoming user certificate.  |
| **Example:** | |
### Verifying the Server and User Authentication Using Digital Certificates

#### SUMMARY STEPS

1. `enable`
2. `show ip ssh`

#### DETAILED STEPS

**Step 1**  
**enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

**Example:**

```
Device> enable
```

**Step 2**  
**show ip ssh**

Displays the currently configured authentication methods. To confirm the use of certificate-based authentication, ensure that the x509v3-ssh-rsa algorithm is the configured host key algorithm.

**Example:**

```
Device# show ip ssh
SSH Enabled - version 1.99  
Authentication methods:publickey,keyboard-interactive,password
```
Configuration Examples for X.509v3 Certificates for SSH Authentication

Example: Configuring Digital Certificates for Server Authentication

Switch> enable
Switch# configure terminal
Switch(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Switch(config)# ip ssh server certificate profile
Switch(ssh-server-cert-profile)# server
Switch(ssh-server-cert-profile-server)# trustpoint sign trust1
Switch(ssh-server-cert-profile-server)# exit

Example: Configuring Digital Certificate for User Authentication

Switch> enable
Switch# configure terminal
Switch(config)# ip ssh server algorithm authentication publickey
Switch(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Switch(config)# ip ssh server certificate profile
Switch(ssh-server-cert-profile)# user
Switch(ssh-server-cert-profile-user)# trustpoint verify trust2
Switch(ssh-server-cert-profile-user)# end

Additional References for X.509v3 Certificates for SSH Authentication

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI configuration</td>
<td>Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature Information for X.509v3 Certificates for SSH Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
The X.509v3 Certificates for SSH Authentication feature uses the X.509v3 digital certificates in server and user authentication at the SSH server side.

The following commands were introduced or modified: `ip ssh server algorithm hostkey`, `ip ssh server algorithm authentication`, and `ip ssh server certificate profile`.

This feature was implemented on the following platforms:

- Catalyst 2960C, 2960CX, 2960P, 2960X, and 2960XR Series Switches
- Catalyst 3560CX and 3560X Series Switches
- Catalyst 3750X Series Switches
- Catalyst 4500E Sup7-E, Sup7L-E, Sup8-E, and 4500X Series Switches
- Catalyst 4900M, 4900F-E Series Switches

---

**Table 77: Feature Information for X.509v3 Certificates for SSH Authentication**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| X.509v3 Certificates for SSH Authentication      | Cisco IOS 15.2(4)E1 | The X.509v3 Certificates for SSH Authentication feature uses the X.509v3 digital certificates in server and user authentication at the SSH server side. The following commands were introduced or modified: `ip ssh server algorithm hostkey`, `ip ssh server algorithm authentication`, and `ip ssh server certificate profile`. This feature was implemented on the following platforms:  
  - Catalyst 2960C, 2960CX, 2960P, 2960X, and 2960XR Series Switches  
  - Catalyst 3560CX and 3560X Series Switches  
  - Catalyst 3750X Series Switches  
  - Catalyst 4500E Sup7-E, Sup7L-E, Sup8-E, and 4500X Series Switches  
  - Catalyst 4900M, 4900F-E Series Switches |
Feature Information for X.509v3 Certificates for SSH Authentication
CHAPTER 40

Configuring Secure Socket Layer HTTP

This feature provides Secure Socket Layer (SSL) version 3.0 support for the HTTP 1.1 server and HTTP 1.1 client within Cisco IOS software. SSL provides server authentication, encryption, and message integrity to allow secure HTTP communications. SSL also provides HTTP client authentication. HTTP over SSL is abbreviated as HTTPS.

- Finding Feature Information, on page 703
- Information About Secure Socket Layer HTTP, on page 703
- Monitoring Secure HTTP Server and Client Status, on page 713
- Configuration Examples for Secure Socket Layer HTTP, on page 713
- Additional References for Secure Socket Layer HTTP, on page 714
- Feature Information for Secure Socket Layer HTTP, on page 715
- Glossary, on page 715

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Secure Socket Layer HTTP

Secure HTTP Servers and Clients Overview

On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser. Cisco's implementation of the secure HTTP server and secure HTTP client uses an implementation of SSL Version 3.0 with application-layer encryption. HTTP over SSL is abbreviated as HTTPS; the URL of a secure connection begins with https:// instead of http://.
SSL evolved into Transport Layer Security (TLS) in 1999, but is still used in this particular context.

The primary role of the HTTP secure server (the switch) is to listen for HTTPS requests on a designated port (the default HTTPS port is 443) and pass the request to the HTTP 1.1 Web server. The HTTP 1.1 server processes requests and passes responses (pages) back to the HTTP secure server, which, in turn, responds to the original request.

The primary role of the HTTP secure client (the web browser) is to respond to Cisco IOS application requests for HTTPS User Agent services, perform HTTPS User Agent services for the application, and pass the response back to the application.

Certificate Authority Trustpoints

Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as trustpoints.

When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client. The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate.

For secure HTTP connections, we highly recommend that you configure a CA trustpoint. If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing).

If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated.

- If the switch is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary self-signed certificate is assigned.

- If the switch has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the switch or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

The certificate authorities and trustpoints must be configured on each device individually. Copying them from other devices makes them invalid on the switch.

When a new certificate is enrolled, the new configuration change is not applied to the HTTPS server until the server is restarted. You can restart the server using either the CLI or by physical reboot. On restarting the server, the switch starts using the new certificate.

If a self-signed certificate has been generated, this information is included in the output of the show running-config privileged EXEC command. This is a partial sample output from that command displaying a self-signed certificate.
Switch# show running-config
Building configuration...

<output truncated>
crypto pki trustpoint TP-self-signed-3080755072
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-3080755072
    revocation-check none
    rsakeypair TP-self-signed-3080755072
!
crypto ca certificate chain TP-self-signed-3080755072
    certificate self-signed 01
        3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
        59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
        6966963 6174652D 33033033 00000000 00000000 300D0609 2A864886 F70D0109
        02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
        30333031 30303030 35395A17 0D323030 31303030 305A3059 312F302D
<output truncated>

You can remove this self-signed certificate by disabling the secure HTTP server and entering the **no crypto pki trustpoint TP-self-signed-30890755072** global configuration command. If you later re-enable a secure HTTP server, a new self-signed certificate is generated.

---

**Note**

The values that follow `TP self-signed` depend on the serial number of the device.

You can use an optional command (**ip http secure-client-auth**) to allow the HTTPS server to request an X.509v3 certificate from the client. Authenticating the client provides more security than server authentication by itself.

---

**CipherSuites**

A CipherSuite specifies the encryption algorithm and the digest algorithm to use on a SSL connection. When connecting to the HTTPS server, the client Web browser offers a list of supported CipherSuites, and the client and server negotiate the best encryption algorithm to use from those on the list that are supported by both. For example, Netscape Communicator 4.76 supports U.S. security with RSA Public Key Cryptography, MD2, MD5, RC2-CBC, RC4, DES-CBC, and DES-EDE3-CBC.

For the best possible encryption, you should use a client browser that supports 128-bit encryption, such as Microsoft Internet Explorer Version 5.5 (or later) or Netscape Communicator Version 4.76 (or later). The SSL_RSA_WITH_DES_CBC_SHA CipherSuite provides less security than the other CipherSuites, as it does not offer 128-bit encryption.

The more secure and more complex CipherSuites require slightly more processing time. This list defines the CipherSuites supported by the switch and ranks them from fastest to slowest in terms of router processing load (speed):

1. **SSL_RSA_WITH_DES_CBC_SHA**—RSA key exchange (RSA Public Key Cryptography) with DES-CBC for message encryption and SHA for message digest
2. **SSL_RSA_WITH_NULL_SHA** key exchange with NULL for message encryption and SHA for message digest (only for SSL 3.0).
3. SSL_RSA_WITH_NULL_MD5 key exchange with NULL for message encryption and MD5 for message digest (only for SSL 3.0).
4. SSL_RSA_WITH_RC4_128_MD5—RSA key exchange with RC4 128-bit encryption and MD5 for message digest
5. SSL_RSA_WITH_RC4_128_SHA—RSA key exchange with RC4 128-bit encryption and SHA for message digest
6. SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest
7. SSL_RSA_WITH_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest (only for SSL 3.0).
8. SSL_RSA_WITH_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).
9. SSL_RSA_WITH_DHE_AES_128_CBC_SHA—RSA key exchange with AES 128-bit encryption and SHA for message digest (only for SSL 3.0).
10. SSL_RSA_WITH_DHE_AES_256_CBC_SHA—RSA key exchange with AES 256-bit encryption and SHA for message digest (only for SSL 3.0).

Note
The latest versions of Chrome do not support the four original cipher suites, thus disallowing access to both web GUI and guest portals.

RSA (in conjunction with the specified encryption and digest algorithm combinations) is used for both key generation and authentication on SSL connections. This usage is independent of whether or not a CA trustpoint is configured.

Default SSL Configuration

The standard HTTP server is enabled.
SSL is enabled.
No CA trustpoints are configured.
No self-signed certificates are generated.

SSL Configuration Guidelines

When SSL is used in a switch cluster, the SSL session terminates at the cluster commander. Cluster member switches must run standard HTTP.

Before you configure a CA trustpoint, you should ensure that the system clock is set. If the clock is not set, the certificate is rejected due to an incorrect date.
How to Configure Secure Socket Layer HTTP

Configuring the Secure HTTP Server

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP server:

Before you begin

If you are using a certificate authority for certification, you should use the previous procedure to configure the CA trustpoint on the switch before enabling the HTTP server. If you have not configured a CA trustpoint, a self-signed certificate is generated the first time that you enable the secure HTTP server. After you have configured the server, you can configure options (path, access list to apply, maximum number of connections, or timeout policy) that apply to both standard and secure HTTP servers.

To verify the secure HTTP connection by using a Web browser, enter https://URL, where the URL is the IP address or hostname of the server switch. If you configure a port other than the default port, you must also specify the port number after the URL. For example:

- https://209.165.129:1026
- https://host.domain.com:1026

Note

AES256_SHA2 is not supported.

SUMMARY STEPS

1. show ip http server status
2. configure terminal
3. ip http secure-server
4. ip http secure-port port-number
5. ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}
6. ip http secure-client-auth
7. ip http secure-trustpoint name
8. ip http path path-name
9. ip http access-class access-list-number
10. ip http max-connections value
11. ip http timeout-policy idle seconds life seconds requests value
12. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> show ip http server status</td>
<td>(Optional) Displays the status of the HTTP server to determine if the secure HTTP server feature is supported in the software. You should see one of these lines in the output:</td>
</tr>
<tr>
<td>Example:</td>
<td>HTTP secure server capability: Present</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>HTTP secure server capability: Not present</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip http secure-server</td>
<td>Enables the HTTPS server if it has been disabled. The HTTPS server is enabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip http secure-port <em>port-number</em></td>
<td>(Optional) Specifies the port number to be used for the HTTPS server. The default port number is 443. Valid options are 443 or any number in the range 1025 to 65535.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip http secure-ciphersuite <em>3des-ede-cbc-sha</em></td>
<td>(Optional) Specifies the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particularly CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.</td>
</tr>
<tr>
<td>[rc4-128-md5] [rc4-128-sha] [des-cbc-sha]]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ip http secure-client-auth</td>
<td>(Optional) Configures the HTTP server to request an X.509v3 certificate from the client for authentication during the connection process. The default is for the client to request a certificate from the server, but the server does not attempt to authenticate the client.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>ip http secure-trustpoint name</code></td>
<td>Specifies the CA trustpoint to use to get an X.509v3 security certificate and to authenticate the client certificate connection. <strong>Note</strong> Use of this command assumes you have already configured a CA trustpoint according to the previous procedure.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ip http secure-trustpoint your_trustpoint</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>ip http path path-name</code></td>
<td>(Optional) Sets a base HTTP path for HTML files. The path specifies the location of the HTTP server files on the local system (usually located in system flash memory).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ip http path /your_server:80</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>ip http access-class access-list-number</code></td>
<td>(Optional) Specifies an access list to use to allow access to the HTTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ip http access-class 2</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>ip http max-connections value</code></td>
<td>(Optional) Sets the maximum number of concurrent connections that are allowed to the HTTP server. We recommend that the value be at least 10 and not less. This is required for the UI to function as expected.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ip http max-connections 4</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>ip http timeout-policy idle seconds life seconds requests value</code></td>
<td>(Optional) Specifies how long a connection to the HTTP server can remain open under the defined circumstances:</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ip http timeout-policy idle 120 life 240 requests 1</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Secure HTTP Client

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP client:

Before you begin

The standard HTTP client and secure HTTP client are always enabled. A certificate authority is required for secure HTTP client certification. This procedure assumes that you have previously configured a CA trustpoint on the switch. If a CA trustpoint is not configured and the remote HTTPS server requires client authentication, connections to the secure HTTP client fail.

**SUMMARY STEPS**

1. `configure terminal`
2. `ip http client secure-trustpoint name`
3. `ip http client secure-ciphersuite {3des-ede-cbc-sha [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip http client secure-trustpoint name</code></td>
<td>(Optional) Specifies the CA trustpoint to be used if the remote HTTP server requests client authentication. Using this command assumes that you have already configured a CA trustpoint by using the previous procedure. The command is optional if client authentication is not needed or if a primary trustpoint has been configured.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# ip http client secure-trustpoint your_trustpoint</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip http client secure-ciphersuite {3des-ede-cbc-sha [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}</code></td>
<td>(Optional) Specifies the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particular CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# ip http client secure-ciphersuite rc4-128-md5</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring a CA Trustpoint

For secure HTTP connections, we recommend that you configure an official CA trustpoint. A CA trustpoint is more secure than a self-signed certificate.

Beginning in privileged EXEC mode, follow these steps to configure a CA Trustpoint:

### SUMMARY STEPS

1. configure terminal
2. hostname hostname
3. ip domain-name domain-name
4. crypto key generate rsa
5. crypto ca trustpoint name
6. enrollment url url
7. enrollment http-proxy host-name port-number
8. crl query url
9. primary name
10. exit
11. crypto ca authentication name
12. crypto ca enroll name
13. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the hostname of the switch (required only if you have not previously configured a hostname). The hostname is required for security keys and certificates.</td>
</tr>
<tr>
<td>hostname hostname</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# hostname your_hostname</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the IP domain name of the switch (required only if you have not previously configured an IP domain name). The domain name is required for security keys and certificates.</td>
</tr>
<tr>
<td>ip domain-name domain-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip domain-name your_domain</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Generates an RSA key pair. RSA key pairs are required before you can obtain a certificate for the switch. RSA key pairs are generated automatically. You can use this command to regenerate the keys, if needed.</td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 5** | **crypto ca trustpoint** *name*  
**Example:**  
`Switch(config)# crypto ca trustpoint your_trustpoint` | Specifies a local configuration name for the CA trustpoint and enter CA trustpoint configuration mode. |
| **Step 6** | **enrollment url** *url*  
**Example:**  
`Switch(ca-trustpoint)# enrollment url http://your_server:80` | Specifies the URL to which the switch should send certificate requests. |
| **Step 7** | **enrollment http-proxy** *host-name* *port-number*  
**Example:**  
`Switch(ca-trustpoint)# enrollment http-proxy your_host 49` | (Optional) Configures the switch to obtain certificates from the CA through an HTTP proxy server.  
- For *host-name*, specify the proxy server used to get the CA.  
- For *port-number*, specify the port number used to access the CA. |
| **Step 8** | **crl query** *url*  
**Example:**  
`Switch(ca-trustpoint)# crl query ldap://your_host:49` | Configures the switch to request a certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked. |
| **Step 9** | **primary** *name*  
**Example:**  
`Switch(ca-trustpoint)# primary your_trustpoint` | (Optional) Specifies that the trustpoint should be used as the primary (default) trustpoint for CA requests.  
- For *name*, specify the trustpoint that you just configured. |
| **Step 10** | **exit**  
**Example:**  
`Switch(ca-trustpoint)# exit` | Exits CA trustpoint configuration mode and return to global configuration mode. |
| **Step 11** | **crypto ca authentication** *name*  
**Example:**  
`Switch(config)# crypto ca authentication your_trustpoint` | Authenticates the CA by getting the public key of the CA. Use the same name used in Step 5. |
Purpose

Command or Action | Purpose
-----------------|---------------------------------------------------------------
**Step 12** crypto ca enroll *name* | Obtains the certificate from the specified CA trustpoint. This command requests a signed certificate for each RSA key pair.
Example:
Switch(config)# crypto ca enroll your_trustpoint

**Step 13** end | Returns to privileged EXEC mode.
Example:
Switch(config)# end

Monitoring Secure HTTP Server and Client Status

To monitor the SSL secure server and client status, use the privileged EXEC commands in the following table.

**Table 78: Commands for Displaying the SSL Secure Server and Client Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip http client secure status</td>
<td>Shows the HTTP secure client configuration.</td>
</tr>
<tr>
<td>show ip http server secure status</td>
<td>Shows the HTTP secure server configuration.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Shows the generated self-signed certificate for secure HTTP connections.</td>
</tr>
</tbody>
</table>

Configuration Examples for Secure Socket Layer HTTP

**Example: Configuring Secure Socket Layer HTTP**

The following example shows a configuration session in which the secure HTTP server is enabled, the port for the secure HTTP server is configured as 1025, and the remote CA trustpoint server “CA-trust-local” is used for certification.

```
Device# show ip http server status
HTTP server status: Disabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path:
Maximum number of concurrent server connections allowed: 5
Server idle time-out: 600 seconds
Server life time-out: 600 seconds
Maximum number of requests allowed on a connection: 1
HTTP secure server capability: Present
HTTP secure server status: Disabled
HTTP secure server port: 443
```
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:

```
Device# configure terminal
Device(config)# ip http secure-server
Device(config)# ip http client secure-trustpoint CA-trust-local
Device(config)# ip http secure-port 1024
Invalid secure port value.
Device(config)# ip http secure-port 1025
Device(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
Device(config)# end
```

```
Device# show ip http serversecure status
HTTP secure server status: Enabled
HTTP secure server port: 1025
HTTP secure server ciphersuite: rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

In the following example, the CA trustpoint CA-trust-local is specified, and the HTTPS client is configured to use this trustpoint for client authentication requests:

```
Device# config terminal
Device(config)# crypto ca trustpoint CA-trust-local
Device(ca-trustpoint)# enrollment url http://example.com
Device(ca-trustpoint)# crl query ldap://example.com
Device(ca-trustpoint)# primary
Device(ca-trustpoint)# exit
Device(config)# ip http client secure-trustpoint CA-trust-local
Device(config)# end
Device# copy running-config startup-config
```

**Additional References for Secure Socket Layer HTTP**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Command List, All Releases</em></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for Secure Socket Layer HTTP

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
<tr>
<td></td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

Glossary

**RSA**—RSA is a widely used Internet encryption and authentication system that uses public and private keys for encryption and decryption. The RSA algorithm was invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman. The abbreviation RSA comes from the first letter of the last names of the three original developers. The RSA algorithm is included in many applications, such as the web browsers from Microsoft and Netscape. The RSA encryption system is owned by RSA Security.

**SHA** — The Secure Hash Algorithm. SHA was developed by NIST and is specified in the Secure Hash Standard (SHS, FIPS 180). Often used as an alternative to Digest 5 algorithm.

**signatures, digital** — In the context of SSL, “signing” means to encrypt with a private key. In digital signing, one-way hash functions are used as input for a signing algorithm. In RSA signing, a 36-byte structure of two hashes (one SHA and one MD5) is signed (encrypted with the private key).

**SSL 3.0** — Secure Socket Layer version 3.0. SSL is a security protocol that provides communications privacy over the Internet. The protocol allows client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. SSL uses a program layer located between the Internet’s HTTP and TCP layers. SSL is included as part of most web server products and as part of most Internet browsers. The SSL 3.0 specification can be found at https://tools.ietf.org/html/rfc6101.
CHAPTER 41

Certification Authority Interoperability

This chapter describes how to configure certification authority (CA) interoperability, which is provided in support of the IPSec protocol. CA interoperability permits Cisco IOS devices and CAs to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPSec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPSec.

• Finding Feature Information, on page 717
• Prerequisites For Certification Authority, on page 717
• Restrictions for Certification Authority, on page 717
• Information About Certification Authority, on page 718
• How to Configure Certification Authority, on page 721
• Monitoring and Maintaining Certification Authority, on page 728

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites For Certification Authority

You need to have a certification authority (CA) available to your network before you configure this interoperability feature. The CA must support the Public Key Infrastructure (PKI) protocol, and the Simple Certificate Enrollment Protocol (SCEP).

Restrictions for Certification Authority

When configuring your CA, the following restrictions apply:
• This feature should be configured only when you also configure both IPsec and Internet Key Exchange (IKE) in your network.
• The Cisco IOS software does not support CA server public keys greater than 2048 bits.

Information About Certification Authority

CA Supported Standards

Without certification authority (CA) interoperability, Cisco IOS devices could not use CAs when deploying IPsec. CAs provide a manageable, scalable solution for IPsec networks.

Cisco supports the following standards with this feature:

• IPSec—IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer; it uses Internet Key Exchange to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.
• Internet Key Exchange (IKE)—A hybrid protocol that implements Oakley and Skeme key exchanges inside the Internet Security Association Key Management Protocol (ISAKMP) framework. Although IKE can be used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.
• Public-Key Cryptography Standard #7 (PKCS #7)—A standard from RSA Data Security, Inc., used to encrypt and sign certificate enrollment messages.
• Public-Key Cryptography Standard #10 (PKCS #10)—A standard syntax from RSA Data Security, Inc. for certificate requests.
• RSA Keys—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA keys come in pairs: one public key and one private key.
• X.509v3 certificates—Certificate support that allows the IPsec-protected network to scale by providing the equivalent of a digital ID card to each device. When two devices wish to communicate, they exchange digital certificates to prove their identity (thus removing the need to manually exchange public keys with each peer or to manually specify a shared key at each peer). These certificates are obtained from a CA. X.509 is part of the X.500 standard of the ITU.

Purpose of CAs

Certificate authorities (CAs) are responsible for managing certificate requests and issuing certificates to participating IPsec network devices. These services provide centralized key management for the participating devices.

CAs simplify the administration of IPsec network devices. You can use a CA with a network containing multiple IPsec-compliant devices such as routers.

Digital signatures, enabled by public key cryptography, provide a means of digitally authenticating devices and individual users. In public key cryptography, such as the RSA encryption system, each user has a key pair containing both a public and a private key. The keys act as complements, and anything encrypted with one of the keys can be decrypted with the other. In simple terms, a signature is formed when data is encrypted with a user's private key. The receiver verifies the signature by decrypting the message with the sender's public
key. The fact that the message could be decrypted using the sender's public key indicates that the holder of the private key, the sender, must have created the message. This process relies on the receiver's having a copy of the sender's public key and knowing with a high degree of certainty that it really does belong to the sender and not to someone pretending to be the sender.

Digital certificates provide the link. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department, or IP address. It also contains a copy of the entity's public key. The certificate is itself signed by a certification authority (CA), a third party that is explicitly trusted by the receiver to validate identities and to create digital certificates.

In order to validate the signature of the CA, the receiver must first know the CA's public key. Normally this process is handled out-of-band or through an operation done at installation. For instance, most web browsers are configured with the public keys of several CAs by default. The Internet Key Exchange (IKE), an essential component of IPSec, can use digital signatures to scalably authenticate peer devices before setting up security associations.

Without digital signatures, one must manually exchange either public keys or secrets between each pair of devices that use IPSec to protect communications between them. Without certificates, every new device added to the network requires a configuration change on every other device with which it communicates securely. With digital certificates, each device is enrolled with a certification authority. When two devices wish to communicate, they exchange certificates and digitally sign data to authenticate each other. When a new device is added to the network, one simply enrolls that device with a CA, and none of the other devices needs modification. When the new device attempts an IPSec connection, certificates are automatically exchanged and the device can be authenticated.

Implementing IPsec Without CAs

Without a CA, if you want to enable IPSec services (such as encryption) between two Cisco devices, you must first ensure that each device has the key of the other device (such as an RSA public key or a shared key). This requirement means that you must manually perform one of the following operations:

- At each device, enter the RSA public key of the other device.
- At each device, specify a shared key to be used by both device.

In the above illustration, each device uses the key of the other device to authenticate the identity of the other device; this authentication always occurs when IPSec traffic is exchanged between the two devices.

If you have multiple Cisco devices in a mesh topology and wish to exchange IPSec traffic passing among all of those devices, you must first configure shared keys or RSA public keys among all of those devices.

Every time a new device is added to the IPSec network, you must configure keys between the new device and each of the existing devices. (In Figure 34, four additional two-part key configurations would be required to add a single encrypting device to the network.)

Consequently, the more devices there are that require IPSec services, the more involved the key administration becomes. This approach does not scale well for larger, more complex encrypting networks.

Implementing IPsec With CAs

With a CA, you do not have to configure keys between all the encrypting devices. Instead, you individually enroll each participating device with the CA, requesting a certificate for the device. When this has been accomplished, each participating device can dynamically authenticate all the other participating devices. This process is illustrated in the illustration.
To add a new IPsec device to the network, you need only configure that new device to request a certificate from the CA, instead of making multiple key configurations with all the other existing IPsec devices.

**Implementing IPsec with Multiple Root CAs**

With multiple root CAs, you no longer have to enroll a device with the CA that issued a certificate to a peer. Instead, you configure a device with multiple CAs that it trusts. Thus, a device can use a configured CA (a trusted root) to verify certificates offered by a peer that were not issued by the same CA defined in the identity of the device.

Configuring multiple CAs allows two or more devices enrolled under different domains (different CAs) to verify the identity of each other when using IKE to set up IPsec tunnels.

Through Simple Certificate Enrollment Protocol (SCEP), each device is configured with a CA (the enrollment CA). The CA issues a certificate to the device that is signed with the private key of the CA. To verify the certificates of peers in the same domain, the device is also configured with the root certificate of the enrollment CA.

To verify the certificate of a peer from a different domain, the root certificate of the enrollment CA in the domain of the peer must be configured securely in the device.

During Internet Key Exchange (IKE) phase one signature verification, the initiator will send the responder a list of its CA certificates. The responder should send the certificate issued by one of the CAs in the list. If the certificate is verified, the device saves the public key contained in the certificate on its public key ring.

With multiple root CAs, VPN users can establish trust in one domain and easily and securely distribute it to other domains. Thus, the required private communication channel between entities authenticated under different domains can occur.

**How CA Certificates Are Used by IPsec Devices**

When two IPsec devices want to exchange IPsec-protected traffic passing between them, they must first authenticate each other—otherwise, IPsec protection cannot occur. The authentication is done with IKE.

Without a CA, a device authenticates itself to the remote device using either RSA-encrypted nonces or preshared keys. Both methods require that keys must have been previously configured between the two devices.

With a CA, a device authenticates itself to the remote device by sending a certificate to the remote device and performing some public key cryptography. Each device must send its own unique certificate that was issued and validated by the CA. This process works because the certificate of each device encapsulates the public key of the device, each certificate is authenticated by the CA, and all participating devices recognize the CA as an authenticating authority. This scheme is called IKE with an RSA signature.

Your device can continue sending its own certificate for multiple IPsec sessions, and to multiple IPsec peers until the certificate expires. When its certificate expires, the device administrator must obtain a new one from the CA.

CAs can also revoke certificates for devices that will no longer participate in IPsec. Revoked certificates are not recognized as valid by other IPsec devices. Revoked certificates are listed in a certificate revocation list (CRL), which each peer may check before accepting a certificate from another peer.
Registration Authorities

Some CAs have a registration authority (RA) as part of their implementation. An RA is essentially a server that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

Some of the configuration tasks described in this document differ slightly, depending on whether your CA supports an RA.

How to Configure Certification Authority

Managing NVRAM Memory Usage

Certificates and certificate revocation lists (CRLs) are used by your device when a CA is used. Normally certain certificates and all CRLs are stored locally in the NVRAM of the device, and each certificate and CRL uses a moderate amount of memory.

The following certificates are normally stored at your device:

- Certificate of your device
- Certificate of the CA
- Root certificates obtained from CA servers (all root certificates are saved in RAM after the device has been initialized)
- Two registration authority (RA) certificates (only if the CA supports an RA)

CRLs are normally stored at your device according to the following conditions:

- If your CA does not support an RA, only one CRL gets stored in the device.
- If your CA supports an RA, multiple CRLs can be stored in the device.

In some cases, storing these certificates and CRLs locally will not present any difficulty. In other cases, memory might become a problem—particularly if the CA supports an RA and a large number of CRLs have to be stored on the device. If the NVRAM is too small to store root certificates, only the fingerprint of the root certificate is saved.

To save NVRAM space, specify that certificates and CRLs should not be stored locally, but should be retrieved from the CA when needed. This alternative will save NVRAM space but could result in a slight performance impact. To specify that certificates and CRLs should not be stored locally on your device, but should be retrieved when required, enable query mode.

If you do not enable query mode now, you can do it later even if certificates and CRLs have are already stored on the device. In this case, when you enable query mode, the stored certificates and CRLs are deleted from the device after you save the configuration. (If you copy the configuration to a TFTP site prior to enabling query mode, you can save any stored certificates and CRLs at the TFTP site.)

Before disabling query mode, perform the copy system:running-config nvramp:startup-config command to save all current certificates and CRLs to NVRAM. Otherwise they could be lost during a reboot.

To specify that certificates and CRLs should not be stored locally on your device, but should be retrieved when required, enable query mode by using the following command in global configuration mode:

```
query mode
```

Query mode may affect availability if the CA is down.
SUMMARY STEPS

1. crypto ca certificate query

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto ca certificate query</td>
<td>Enables query mode, which causes certificates and CRLs not to be stored locally.</td>
</tr>
</tbody>
</table>

Example:
Device(config)# crypto ca certificate query

Configuring the Device Host Name and IP Domain Name

You must configure the host name and IP domain name of a device if this has not already been done. This is required because the device assigns a fully qualified domain name (FQDN) to the keys and certificates used by IPsec, and the FQDN is based on the host name and IP domain name assigned to the device. For example, a certificate named "device20.example.com" is based on a device host name of "device20" and a device IP domain name of "example.com".

SUMMARY STEPS

1. enable
2. configure terminal
3. hostname name
4. ip domain-name name
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname name</td>
<td>Configures the host name of the device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# hostname device1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip domain-name name</td>
<td>Configures the IP domain name of the device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip domain-name domain.com</td>
<td></td>
</tr>
</tbody>
</table>
Generating an RSA Key Pair

Rivest, Shamir, and Adelman (RSA) key pairs are used to sign and encrypt IKE key management messages and are required before obtaining a certificate for your device.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto key generate rsa [usage-keys]
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto key generate rsa [usage-keys]</td>
<td>Generates an RSA key pair.</td>
</tr>
<tr>
<td>Example: Device(config)# crypto key generate rsa usage-keys</td>
<td>• Use the usage-keys keyword to specify special-usage keys instead of general-purpose keys.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits global configuration and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Declaring a Certification Authority**

You should declare one certification authority (CA) to be used by the device.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto ca trustpoint name
4. enrollment url `url`
5. enrollment command
6. exit
7. crypto pki trustpoint `name`
8. crl query ldap://`url`:[`port`]
9. enrollment {mode `ra` | retry count `number` | retry period `minutes` | url `url`}
10. enrollment {mode `ra` | retry count `number` | retry period `minutes` | url `url`}
11. revocation-check `method1` [`method2` `method3`]
12. end

## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto ca trustpoint <code>name</code></td>
<td>Declares the certification authority (CA) that your device should use and enters the CA profile enroll configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# crypto ca trustpoint ka</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enrollment url <code>url</code></td>
<td>Specifies the URL of the CA server to which enrollment requests are sent.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-profile-enroll)# enrollment url <a href="http://entrust:81">http://entrust:81</a></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> enrollment command</td>
<td>Specifies the HTTP command that is sent to the CA for enrollment.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-profile-enroll)# enrollment command</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exit CA profile enroll configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-profile-enroll)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> crypto pki trustpoint <code>name</code></td>
<td>Declares the trustpoint that your device should use and enters Ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# crypto pki trustpoint ka</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> crl query ldap://<code>url</code>:[<code>port</code>]</td>
<td>Queries the certificate revocation list (CRL) to ensure that the certificate of the peer is not revoked.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-trustpoint)# crl query ldap://bar.cisco.com:3899</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Root CA (Trusted Root)

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `crypto ca trustpoint name`
4. `revocation-check method1 [method2 method3]`
5. `root tftp server-hostname filename`
6. `enrollment http-proxy hostname port-number`
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Declares the trustpoint that your device should use and enters CA trustpoint configuration mode.</td>
</tr>
<tr>
<td>crypto ca trustpoint name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Purpose | Command or Action |
--- | --- |
Checks the revocation status of a certificate. | Device(config)# crypto ca trustpoint ka |
Step 4 | revocation-check method1 [method2 method3] |
Example: | Device(ca-trustpoint)# revocation-check ocsp |
Obtains the certification authority (CA) certificate via TFTP. | root tftp server-hostname filename |
Example: | Device(ca-trustpoint)# root tftp server1 file1 |
Accesses the certification authority (CA) by HTTP through the proxy server. | enrollment http-proxy hostname port-number |
Example: | Device(ca-trustpoint)# enrollment http-proxy host2 8080 |
Exits CA trustpoint configuration mode and returns to privileged EXEC mode. | end |
Example: | Device(ca-trustpoint)# end |

**Authenticating the CA**

The device must authenticate the certification authority (CA). It does this by obtaining the self-signed certificate of the CA, which contains the public key of the CA. Because the certificate of the CA is self-signed (the CA signs its own certificate) the public key of the CA should be manually authenticated by contacting the CA administrator to compare the fingerprint of the CA certificate when you perform this step.

Perform the following task to get the public key of the CA:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto pki authenticate
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>

**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.
### Requesting Signed Certificates

You must obtain a signed certificate from the certification authority (CA) for each of the RSA key pairs on your device. If you generated general-purpose RSA keys, your device has only one RSA key pair and needs only one certificate. If you previously generated special-usage RSA keys, your device has two RSA key pairs and needs two certificates.

Perform the following task to request signed certificates from the CA:

---

**Note**

If your device reboots after you have issued the `crypto pki enroll` command, but before you have received the certificates, you must reissue the command and notify the CA administrator.

---

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `crypto pki enroll number`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt;</code> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt;</code> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>crypto pki enroll number</code></td>
<td>Obtains certificates for your device from the CA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device(config)</code> <code>crypto pki enroll myca</code></td>
<td></td>
</tr>
</tbody>
</table>
**Command or Action** | **Purpose**
--- | ---
**Step 4** | **end**
**Example:**
Device(config)# end

Exits global configuration mode and returns to privileged EXEC mode.

---

What to do next

Saving Your Configuration

Always remember to save your work when you make configuration changes.

Use the `copy system:running-config nvram:startup-config` command to save your configuration. This command includes saving RSA keys to private NVRAM. RSA keys are not saved with your configuration when you use a `copy system:running-config rcp` or `copy system:running-config tftp` command.

---

**Monitoring and Maintaining Certification Authority**

**Requesting a Certificate Revocation List**

You can request a certificate revocation list (CRL) only if the certification authority (CA) does not support a registration authority (RA). The following task applies only when the CA does not support an RA.

When a device receives a certificate from a peer, your device will download a CRL from the CA. The device then checks the CRL to make sure the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, the device will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires if query mode is off. If the device receives a peer's certificate after the applicable CRL has expired, the device will download the new CRL.

If the device has a CRL that has not yet expired, but you suspect that the contents of the CRL are out of date, you can request that the latest CRL be downloaded immediately to replace the old CRL.

* 

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `crypto pki crl request name`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
</tbody>
</table>
| **Example:**
Device> enable |

Enables privileged EXEC mode.

* Enter your password if prompted.
Purpose

Command or Action

Step 2 configure terminal

Example:

Device# configure terminal

Purpose

Enters global configuration mode.

Step 3 crypto pki crl request name

Example:

Device(config)# crypto pki crl request myca

Purpose

Requests that a new certificate revocation list (CRL) be obtained immediately from the CA.

Step 4 end

Example:

Device(config)# end

Purpose

Exits global configuration mode and returns to privileged EXEC mode.

Querying a Certification Revocation List

You can query a certificate revocation list (CRL) only when you configure your device with a trusted root. When your device receives a certificate from a peer from another domain (with a different CA), the CRL downloaded from the CA of the device will not include certificate information about the peer. Therefore, you should check the CRL published by the configured root with the LDAP URL to ensure that the certificate of the peer has not been revoked.

If you would like CRL of the root certificate to be queried when the device reboots, you must enter the `crl query` command.

Perform the following task to query the CRL published by the configured root with the LDAP URL:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto pki trustpoint name
4. crl query ldap://url:[port]
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Deleting RSA Keys from a Device

Under certain circumstances you may want to delete RSA keys from your device. For example, if you believe the RSA keys were compromised in some way and should no longer be used, you should delete the keys.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto key zeroize rsa [key-pair-label]`
4. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>crypto key zeroize rsa [key-pair-label]</code></td>
<td>Deletes all Rivest, Shamir, and Adelman (RSA) keys from your device.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# crypto key zeroize rsa</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
What to do next

After you delete RSA keys from the device, you should also complete the following two additional tasks:

- Ask the CA administrator to revoke the device certificates at the CA; you must supply the challenge password that you created when you originally obtained the device certificates with the `crypto pki enroll` command.
- Manually remove the device certificates from the device configuration.

Deleting Public Keys for a Peer

Under certain circumstances you may want to delete RSA public keys of peer devices from your device configuration. For example, if you no longer trust the integrity of the public key of a peer, you should delete the key.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto key pubkey-chain rsa`
4. `no named key key-name [encryption | signature]`
5. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  **Example:**  
  Device> enable |
| Step 2 | `configure terminal` | Enters global configuration mode.  
  **Example:**  
  Device# configure terminal |
| Step 3 | `crypto key pubkey-chain rsa` | Enters public key chain configuration mode, so that you can manually specify other devices’ RSA public keys.  
  **Example:**  
  Device(config)# crypto key pubkey-chain rsa |
| Step 4 | `no named key key-name [encryption | signature]` | Deletes the RSA public key of a remote peer and enters public key configuration mode.  
  **Example:**  
  Device(config-pubkey-c)# no named-key otherpeer.example.com |
| Step 5 | `end` | Exits public key configuration mode and returns to privileged EXEC mode.  
  **Example:**  
  Device(config-pubkey)# end |
Deleting Certificates from the Configuration

If the need arises, you can delete certificates that are saved in your device. Your device saves its own certificates, the certificate of the CA, and any RA certificates.

To delete the CA’s certificate, you must remove the entire CA identity, which also removes all certificates associated with the CA—your router’s certificate, the CA certificate, and any RA certificates.

**SUMMARY STEPS**

1. enable
2. show crypto pki certificates
3. configure terminal
4. crypto pki certificate chain name
5. no certificate certificate-serial-number
6. exit
7. no crypto pki import name certificate
8. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
Example:  
Device> enable  
- Enter your password if prompted. |
| **Step 2** show crypto pki certificates | Displays information about your device certificate, the certification authority (CA) certificate, and any registration authority (RA) certificates.  
Example:  
Device# show crypto pki certificates |
| **Step 3** configure terminal | Enters global configuration mode.  
Example:  
Device# configure terminal |
| **Step 4** crypto pki certificate chain name | Enters certificate chain configuration mode.  
Example:  
Device(config)# crypto pki certificate chain myca |
| **Step 5** no certificate certificate-serial-number | Deletes the certificate.  
Example:  
Device(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF |
| **Step 6** exit | Exits certificate chain configuration mode and returns to global configuration mode.  
Example:  
Device(config-cert-chain)# exit |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> no crypto pki import name certificate</td>
<td>Deletes a certificate manually.</td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Viewing Keys and Certificates

Perform the following task to view keys and certificates:

#### SUMMARY STEPS

1. enable
2. show crypto key mypubkey rsa [keyname]
3. show crypto key pubkey-chain rsa
4. show crypto key pubkey-chain rsa [name key-name | address key-address]
5. show crypto pki certificates
6. show crypto pki trustpoints

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show crypto key mypubkey rsa [keyname]</td>
<td>Displays the RSA public keys configured on a device.</td>
</tr>
<tr>
<td>Example: Device# show crypto key mypubkey rsa [keyname]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show crypto key pubkey-chain rsa</td>
<td>Displays the RSA public keys of the peer that are stored on a device.</td>
</tr>
<tr>
<td>Example: Device# show crypto key pubkey-chain rsa</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show crypto key pubkey-chain rsa [name key-name</td>
<td>address key-address]</td>
</tr>
<tr>
<td>Example: Device# show crypto key pubkey-chain rsa address 209.165.202.129</td>
<td></td>
</tr>
</tbody>
</table>
### Viewing Keys and Certificates

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> show crypto pki certificates</td>
<td>Displays information about the device certificate, the certification authority (CA) certificate, and any registration authority (RA) certificates</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show crypto pki certificates</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show crypto pki trustpoints</td>
<td>Displays trustpoints that are configured on a device.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show crypto pki certificates</td>
<td></td>
</tr>
</tbody>
</table>
Access Control List Overview

Access lists filter network traffic by controlling the forwarding or blocking of packets at the interface of a device. A device examines each packet to determine whether to forward or drop that packet, based on the criteria specified in access lists.

The criteria that can be specified in an access list include the source address of the traffic, the destination address of the traffic, and the upper-layer protocol.

Note

Some users might successfully evade basic access lists because these lists require no authentication.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Access Control Lists

Definition of an Access List

An access list is a sequential list consisting of at least one permit statement and possibly one or more deny statements. In the case of IP access lists, the statements can apply to IP addresses, upper-layer IP protocols, or other fields in IP packets. The access list is identified and referenced by a name or a number. Access list acts as a packet filter, filtering packets based on the criteria defined in the access list.
An access list may be configured, but it does not take effect until the access list is either applied to an interface, a virtual terminal line (vt), or referenced by some command that accepts an access list. Multiple commands can reference the same access list.

The following configuration example shows how to create an IP access list named branchoffices. The ACL is applied to serial interface 0/gigabitEthernet on incoming packets. No sources other than those on the networks specified by each source address and mask pair can access this interface. The destinations for packets coming from sources on network 172.20.7.0 are unrestricted. The destination for packets coming from sources on network 172.29.2.0 must be 172.25.5.4.

```plaintext
ip access-list extended branchoffices
10 permit 172.20.7.0 0.0.0.3 any
20 permit 172.29.2.0 0.0.0.255 host 172.25.5.4
!
interface serial 0
ip access-group branchoffices in

ip access-list extended branchoffices
10 permit 172.20.7.0 0.0.0.3 any
20 permit 172.29.2.0 0.0.0.255 host 172.25.5.4
!
gigabitEthernet 0/1
ip access-group branchoffices in
```

**Functions of an Access Control List**

There are many reasons to configure access lists; for example, to restrict contents of routing updates or to provide traffic flow control. One of the most important reasons to configure access lists is to provide security for your network, which is the focus of this module.

Use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your device, all packets passing through the device are allowed access to all parts of your network.

Access lists can allow a host to access a part of your network and prevent another host from accessing the same area. In the figure below, Host A is allowed to access the Human Resources network, but Host B is prevented from accessing the Human Resources network.

You can also use access lists to define the type of traffic that is forwarded or blocked at device interfaces. For example, you can permit e-mail traffic to be routed but at the same time block all Telnet traffic.

**Purpose of IP Access Lists**

Access lists perform packet filtering to control which packets move through the network and where. Such control can help limit network traffic and restrict the access of users and devices to the network. Access lists have many uses, and therefore many commands accept a reference to an access list in their command syntax.

Access lists can be used to do the following:

- Filter incoming packets on an interface.
- Filter outgoing packets on an interface.
- Limit debug output based on an address or protocol.
- Control virtual terminal line access.
• Identify or classify traffic for advanced features, such as congestion avoidance, congestion management, and priority and custom queuing.

**Reasons to Configure ACLs**

There are many reasons to configure access lists; for example, you can use access lists to restrict contents of switching updates or to provide traffic flow control. One of the most important reasons to configure access lists is to provide a basic level of security for your network by controlling access to it. If you do not configure access lists on your device, all packets passing through the device could be allowed onto all parts of your network.

An access list can allow one host to access a part of your network and prevent another host from accessing the same area. For example, by applying an appropriate access list to interfaces of a device, Host A is allowed to access the human resources network and Host B is prevented from accessing the human resources network.

You can use access lists on a device that is positioned between two parts of your network, to control traffic entering or exiting a specific part of your internal network.

To provide some security benefits of access lists, you should at least configure access lists on border devices—devices located at the edges of your networks. Such an access list provides a basic buffer from the outside network or from a less controlled area of your own network into a more sensitive area of your network.

On these border devices, you should configure access lists for each network protocol configured on the device interfaces. You can configure access lists so that inbound traffic or outbound traffic or both are filtered on an interface.

Access lists are defined on a per-protocol basis. In other words, you should define access lists for every protocol enabled on an interface if you want to control traffic flow for that protocol.

**Software Processing of an Access List**

The following general steps describe how the an access list is processed when it is applied to an interface, a vty, or referenced by any command. These steps apply to an access list that has 13 or fewer access list entries.

• The software receives an IP packet and tests parts of each packet being filtered against the conditions in the access list, one condition (permit or deny statement) at a time. For example, the software tests the source and destination addresses of the packet against the source and destination addresses in a permit or deny statement.

• If a packet does not match an access list statement, the packet is then tested against the next statement in the list.

• If a packet and an access list statement match, the rest of the statements in the list are skipped and the packet is permitted or denied as specified in the matched statement. The first entry that the packet matches determines whether the software permits or denies the packet. That is, after the first match, no subsequent entries are considered.

• If no conditions match, the software drops the packet. This is because each access list ends with an unwritten, implicit deny statement. That is, if the packet has not been permitted by the time it was tested against each statement, it is denied.

An access list with more than 13 entries is processed using a trie-based lookup algorithm. This process will happen automatically; it does not need to be configured.
Access List Rules

The following rules apply to access control lists (ACLs):

- Only one access list per interface, per protocol, and per direction is allowed.
- An access list must contain at least one permit statement or all packets are denied entry into the network.
- The order in which access list conditions or match criteria are configured is important. While deciding whether to forward or block a packet, Cisco software tests the packet against each criteria statement in the order in which these statements are created. After a match is found, no more criteria statements are checked. The same permit or deny statements specified in a different order can result in a packet being passed under one circumstance and denied in another circumstance.
- If an access list is referenced by a name, but the access list does not exist, all packets pass. An interface or command with an empty access list applied to it permits all traffic into the network.
- Standard access lists and extended access lists cannot have the same name.
- Inbound access lists process packets before packets are sent to an outbound interface. Inbound access lists that have filtering criteria that deny packet access to a network saves the overhead of a route lookup. Packets that are permitted access to a network based on the configured filtering criteria are processed for routing. For inbound access lists, when you configure a permit statement, packets are processed after they are received, and when you configure a deny statement, packets are discarded.
- Outbound access lists process packets before they leave the device. Incoming packets are routed to the outbound interface and then processed by the outbound access list. For outbound access lists, when you configure a permit statement, packets are sent to the output buffer, and when you configure a deny statement, packets are discarded.
- An access list can control traffic arriving at a device or leaving a device, but not traffic originating at a device.

Helpful Hints for Creating IP Access Lists

The following tips will help you avoid unintended consequences and help you create more efficient access lists.

- Create the access list before applying it to an interface (or elsewhere), because if you apply a nonexistent access list to an interface and then proceed to configure the access list, the first statement is put into effect, and the implicit deny statement that follows could cause you immediate access problems.
- Another reason to configure an access list before applying it is because an interface with an empty access list applied to it permits all traffic.
- All access lists need at least one permit statement; otherwise, all packets are denied and no traffic passes.
- Because the software stops testing conditions after it encounters the first match (to either a permit or deny statement), you will reduce processing time and resources if you put the statements that packets are most likely to match at the beginning of the access list. Place more frequently occurring conditions before less frequent conditions.
- Organize your access list so that more specific references in a network or subnet appear before more general ones.
• Use the statement `permit any any` if you want to allow all other packets not already denied. Using the statement `permit any any` in effect avoids denying all other packets with the implicit deny statement at the end of an access list. Do not make your first access list entry `permit any any` because all traffic will get through; no packets will reach the subsequent testing. In fact, once you specify `permit any any`, all traffic not already denied will get through.

• Although all access lists end with an implicit `deny` statement, we recommend use of an explicit `deny` statement (for example, `deny ip any any`). On most platforms, you can display the count of packets denied by issuing the `show access-list` command, thus finding out more information about who your access list is disallowing. Only packets denied by explicit `deny` statements are counted, which is why the explicit `deny` statement will yield more complete data for you.

• While you are creating an access list or after it is created, you might want to delete an entry.
  - You cannot delete an entry from a numbered access list; trying to do so will delete the entire access list. If you need to delete an entry, you need to delete the entire access list and start over.
  - You can delete an entry from a named access list. Use the `no permit` or `no deny` command to delete the appropriate entry.

• In order to make the purpose of individual statements more scannable and easily understood at a glance, you can write a helpful remark before or after any statement by using the `remark` command.

• If you want to deny access to a particular host or network and find out if someone from that network or host is attempting to gain access, include the `log` keyword with the corresponding `deny` statement so that the packets denied from that source are logged for you.

• This hint applies to the placement of your access list. When trying to save resources, remember that an inbound access list applies the filter conditions before the routing table lookup. An outbound access list applies the filter conditions after the routing table lookup.

**IP Packet Fields You Can Filter to Control Access**

You can use an extended access list to filter on any of the following fields in an IP packet. Source address and destination address are the two most frequently specified fields on which to base an access list:

• Source address--Specifies a source address to control packets coming from certain networking devices or hosts.

• Destination address--Specifies a destination address to control packets being sent to certain networking devices or hosts.

**Source and Destination Addresses**

Source and destination address fields in an IP packet are two typical fields on which to base an access list. Specify source addresses to control the packets being sent from certain networking devices or hosts. Specify destination addresses to control the packets being sent to certain networking devices or hosts.
Wildcard Mask for Addresses in an Access List

Address filtering uses wildcard masking to indicate to the software whether to check or ignore corresponding IP address bits when comparing the address bits in an access list entry to a packet being submitted to the access list. By carefully setting wildcard masks, you can specify one or more IP addresses for permit or deny tests.

Wildcard masking for IP address bits uses the number 1 and the number 0 to specify how the software treats the corresponding IP address bits. A wildcard mask is sometimes referred to as an inverted mask because a 1 and 0 mean the opposite of what they mean in a subnet (network) mask.

- A wildcard mask bit 0 means check the corresponding bit value; they must match.
- A wildcard mask bit 1 means ignore that corresponding bit value; they need not match.

If you do not supply a wildcard mask with a source or destination address in an access list statement, the software assumes an implicit wildcard mask of 0.0.0.0, meaning all values must match.

Unlike subnet masks, which require contiguous bits indicating network and subnet to be ones, wildcard masks allow noncontiguous bits in the mask.

The table below shows examples of IP addresses and masks from an access list, along with the corresponding addresses that are considered a match.

**Table 78: Sample IP Addresses, Wildcard Masks, and Match Results**

<table>
<thead>
<tr>
<th>Address</th>
<th>Wildcard Mask</th>
<th>Match Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
<td>All addresses will match the access list conditions.</td>
</tr>
<tr>
<td>172.18.0.0/16</td>
<td>0.0.255.255</td>
<td>Network 172.18.0</td>
</tr>
<tr>
<td>172.18.5.2/16</td>
<td>0.0.0.0</td>
<td>Only host 172.18.5.2 matches</td>
</tr>
<tr>
<td>172.18.8.0</td>
<td>0.0.0.7</td>
<td>Only subnet 172.18.8.0/29 matches</td>
</tr>
<tr>
<td>172.18.8.8</td>
<td>0.0.0.7</td>
<td>Only subnet 172.18.8.8/29 matches</td>
</tr>
<tr>
<td>172.18.8.15</td>
<td>0.0.0.3</td>
<td>Only subnet 172.18.8.15/30 matches</td>
</tr>
<tr>
<td>10.1.2.0</td>
<td>0.0.254.255 (noncontiguous bits in mask)</td>
<td>Matches any even-numbered network in the range of 10.1.2.0 to 10.1.254.0</td>
</tr>
</tbody>
</table>

Access List Sequence Numbers

The ability to apply sequence numbers to IP access list entries simplifies access list changes. Prior to the IP Access List Entry Sequence Numbering feature, there was no way to specify the position of an entry within an access list. If you wanted to insert an entry in the middle of an existing list, all of the entries after the desired position had to be removed, then the new entry was added, and then all the removed entries had to be reentered. This method was cumbersome and error prone.

This feature allows users to add sequence numbers to access list entries and resequence them. When you add a new entry, you specify the sequence number so that it is in a desired position in the access list. If necessary, entries currently in the access list can be resequenced to create room to insert the new entry.
ACL Supported Types

The switch supports IP ACLs and Ethernet (MAC) ACLs:

- IP ACLs filter IPv4 traffic, including TCP, User Datagram Protocol (UDP), Internet Group Management Protocol (IGMP), and Internet Control Message Protocol (ICMP).
- Ethernet ACLs filter non-IP traffic.

Supported ACLs

The switch supports three types of ACLs to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply only one IP access list and one MAC access list to a Layer 2 interface.

Port ACLs

Port ACLs are ACLs that are applied to Layer 2 interfaces on a switch. Port ACLs are supported only on physical interfaces and not on EtherChannel interfaces. Port ACLs can be applied to the interface only in inbound direction. The following access lists are supported:

- Standard IP access lists using source addresses
- Extended IP access lists using source and destination addresses and optional protocol type information
- MAC extended access lists using source and destination MAC addresses and optional protocol type information

The switch examines ACLs on an interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL. In this way, ACLs control access to a network or to part of a network.

Figure 52: Using ACLs to Control Traffic in a Network

This is an example of using port ACLs to control access to a network when all workstations are in the same VLAN. ACLs applied at the Layer 2 input would allow Host A to access the Human Resources network, but prevent Host B from accessing the same network. Port ACLs can only be applied to Layer 2 interfaces in the inbound direction.
When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs. With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.

**Note**

You cannot apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

### Access Control Entries

An ACL contains an ordered list of access control entries (ACEs). Each ACE specifies *permit* or *deny* and a set of conditions the packet must satisfy in order to match the ACE. The meaning of *permit* or *deny* depends on the context in which the ACL is used.

### ACEs and Fragmented and Unfragmented Traffic

IP packets can be fragmented as they cross the network. When this happens, only the fragment containing the beginning of the packet contains the Layer 4 information, such as TCP or UDP port numbers, ICMP type and code, and so on. All other fragments are missing this information.

Some access control entries (ACEs) do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.
- Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

### ACEs and Fragmented and Unfragmented Traffic Examples

Consider access list 102, configured with these commands, applied to three fragmented packets:

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

**Note**

In the first and second ACEs in the examples, the *eq* keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.
• Packet A is a TCP packet from host 10.2.2.2, port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.

• Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit). Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

• Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.
Configuring IPv4 Access Control Lists

Access control lists (ACLs) perform packet filtering to control which packets move through the network and where. Such control provides security by helping to limit network traffic, restrict the access of users and devices to the network, and prevent traffic from leaving a network. IP access lists can reduce the chance of spoofing and denial-of-service attacks and allow dynamic, temporary user access through a firewall.

IP access lists can also be used for purposes other than security, such as bandwidth control, limiting debug output, and identifying or classifying traffic for quality of service (QoS) features. This module provides an overview of IP access lists.

- Finding Feature Information, on page 745
- Restrictions for Configuring IPv4 Access Control Lists, on page 745
- Information About Configuring IPv4 Access Control Lists, on page 746
- How to Configure ACLs, on page 754
- Monitoring IPv4 ACLs, on page 771
- Configuration Examples for ACLs, on page 772
- Examples: Troubleshooting ACLs, on page 779
- Additional References, on page 780
- Feature Information for IPv4 Access Control Lists, on page 780

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring IPv4 Access Control Lists

General Network Security

The following are restrictions for configuring network security with ACLs:
• Router ACL and VLAN ACLs are not supported.

• Not all commands that accept a numbered ACL accept a named ACL. ACLs for packet filters and route filters on interfaces can use a name.

• A standard ACL and an extended ACL cannot have the same name.

• Though visible in the command-line help strings, **appletalk** is not supported as a matching condition for the **deny** and **permit** MAC access-list configuration mode commands.

• ACL wildcard is not supported in downstream client policy.

### IPv4 ACL Network Interfaces

The following restrictions apply to IPv4 ACLs to network interfaces:

• When controlling access to an interface, you can use a named or numbered ACL.

• If you apply an ACL to a Layer 3 interface and routing is not enabled on the switch, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic.

• You do not have to enable routing to apply ACLs to Layer 2 interfaces.

• On Layer 3 ports and SVIs, ACLs are not supported.

### MAC ACLs on a Layer 2 Interface

After you create a MAC ACL, you can apply it to a Layer 2 interface to filter non-IP traffic coming in that interface. When you apply the MAC ACL, consider these guidelines:

• You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface. The IP access list filters only IP packets, and the MAC access list filters non-IP packets.

• A Layer 2 interface can have only one MAC access list. If you apply a MAC access list to a Layer 2 interface that has a MAC ACL configured, the new ACL replaces the previously configured one.

---

**Note**

The `mac access-group` interface configuration command is only valid when applied to a physical Layer 2 interface. You cannot use the command on EtherChannel port channels.

### IP Access List Entry Sequence Numbering

• This feature does not support dynamic, reflexive, or firewall access lists.

---

**Information About Configuring IPv4 Access Control Lists**

**ACL Overview**

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a router or switch and permit or deny packets crossing specified interfaces or
VLANs. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards, including packets bridged within a VLAN.

You configure access lists on a router or Layer 3 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both.

**Standard and Extended IPv4 ACLs**

This section describes IP ACLs.

An ACL is a sequential collection of permit and deny conditions. One by one, the switch tests packets against the conditions in an access list. The first match determines whether the switch accepts or rejects the packet. Because the switch stops testing after the first match, the order of the conditions is critical. If no conditions match, the switch denies the packet.

The software supports these types of ACLs or access lists for IPv4:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses for matching operations and optional protocol-type information for finer granularity of control.

**IPv4 ACL Switch Unsupported Features**

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers.

The following ACL-related features are not supported:

- Non-IP protocol ACLs or bridge-group ACLs
- IP accounting
- Inbound and outbound rate limiting (except with QoS ACLs)
- Reflexive ACLs and dynamic ACLs are not supported. (except for some specialized dynamic ACLs used by the switch clustering feature)
- ACL logging for VLAN maps

**Access List Numbers**

The number you use to denote your ACL shows the type of access list that you are creating.
This list the access-list number and corresponding access list type and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, numbers 1 to 199 and 1300 to 2699.

Table 80: Access List Numbers

<table>
<thead>
<tr>
<th>Access List Number</th>
<th>Type</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–99</td>
<td>IP standard access list</td>
<td>Yes</td>
</tr>
<tr>
<td>100–199</td>
<td>IP extended access list</td>
<td>Yes</td>
</tr>
<tr>
<td>200–299</td>
<td>Protocol type-code access list</td>
<td>No</td>
</tr>
<tr>
<td>300–399</td>
<td>DECnet access list</td>
<td>No</td>
</tr>
<tr>
<td>400–499</td>
<td>XNS standard access list</td>
<td>No</td>
</tr>
<tr>
<td>500–599</td>
<td>XNS extended access list</td>
<td>No</td>
</tr>
<tr>
<td>600–699</td>
<td>AppleTalk access list</td>
<td>No</td>
</tr>
<tr>
<td>700–799</td>
<td>48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>800–899</td>
<td>IPX standard access list</td>
<td>No</td>
</tr>
<tr>
<td>900–999</td>
<td>IPX extended access list</td>
<td>No</td>
</tr>
<tr>
<td>1000–1099</td>
<td>IPX SAP access list</td>
<td>No</td>
</tr>
<tr>
<td>1100–1199</td>
<td>Extended 48-bit MAC address access list</td>
<td>No</td>
</tr>
<tr>
<td>1200–1299</td>
<td>IPX summary address access list</td>
<td>No</td>
</tr>
<tr>
<td>1300–1999</td>
<td>IP standard access list (expanded range)</td>
<td>Yes</td>
</tr>
<tr>
<td>2000–2699</td>
<td>IP extended access list (expanded range)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

In addition to numbered standard and extended ACLs, you can also create standard and extended named IP ACLs by using the supported numbers. That is, the name of a standard IP ACL can be 1 to 99; the name of an extended IP ACL can be 100 to 199. The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

**Numbered Standard IPv4 ACLs**

When creating an ACL, remember that, by default, the end of the ACL contains an implicit deny statement for all packets that it did not find a match for before reaching the end. With standard access lists, if you omit the mask from an associated IP host address ACL specification, 0.0.0.0 is assumed to be the mask.

The switch always rewrites the order of standard access lists so that entries with **host** matches and entries with matches having a **don’t care** mask of 0.0.0.0 are moved to the top of the list, above any entries with
non-zero don’t care masks. Therefore, in show command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to VLANs, to terminal lines, or to interfaces.

**Numbered Extended IPv4 ACLs**

Although standard ACLs use only source addresses for matching, you can use extended ACL source and destination addresses for matching operations and optional protocol type information for finer granularity of control. When you are creating ACEs in numbered extended access lists, remember that after you create the ACL, any additions are placed at the end of the list. You cannot reorder the list or selectively add or remove ACEs from a numbered list.

The switch does not support dynamic or reflexive access lists. It also does not support filtering based on the type of service (ToS) minimize-monetary-cost bit.

Some protocols also have specific parameters and keywords that apply to that protocol.

You can define an extended TCP, UDP, ICMP, IGMP, or other IP ACL. The switch also supports these IP protocols:

---

**Note**

ICMP echo-reply cannot be filtered. All other ICMP codes or types can be filtered.

These IP protocols are supported:

- Authentication Header Protocol (`ahp`)
- Encapsulation Security Payload (`esp`)
- Enhanced Interior Gateway Routing Protocol (`eigrp`)
- generic routing encapsulation (`gre`)
- Internet Control Message Protocol (`icmp`)
- Internet Group Management Protocol (`igmp`)
- any Interior Protocol (`ip`)
- IP in IP tunneling (`ipinip`)
- KA9Q NOS-compatible IP over IP tunneling (`nos`)
- Open Shortest Path First routing (`ospf`)
- Payload Compression Protocol (`pcp`)
- Protocol-Independent Multicast (`pim`)
- Transmission Control Protocol (`tcp`)
- User Datagram Protocol (`udp`)

**Named IPv4 ACLs**

You can identify IPv4 ACLs with an alphanumeric string (a name) rather than a number. You can use named ACLs to configure more IPv4 access lists in a router than if you were to use numbered access lists. If you
identify your access list with a name rather than a number, the mode and command syntax are slightly different. However, not all commands that use IP access lists accept a named access list.

**Note**

The name you give to a standard or extended ACL can also be a number in the supported range of access list numbers. That is, the name of a standard IP ACL can be 1 to 99 and . The advantage of using named ACLs instead of numbered lists is that you can delete individual entries from a named list.

Consider these guidelines before configuring named ACLs:

- Numbered ACLs are also available.
- A standard ACL and an extended ACL cannot have the same name.
- You can use standard or extended ACLs (named or numbered) in VLAN maps.

**Benefits of Using the Named ACL Support for Noncontiguous Ports on an Access Control Entry Feature**

The Named ACL Support for Noncontiguous Ports on an Access Control Entry feature allows you to specify noncontiguous ports in a single access control entry, which greatly reduces the number of entries required in an access control list when several entries have the same source address, destination address, and protocol, but differ only in the ports.

This feature greatly reduces the number of access control entries (ACEs) required in an access control list to handle multiple entries for the same source address, destination address, and protocol. If you maintain large numbers of ACEs, use this feature to consolidate existing groups of access list entries wherever it is possible and when you create new access list entries. When you configure access list entries with noncontiguous ports, you will have fewer access list entries to maintain.

**Benefits of IP Access List Entry Sequence Numbering**

The ability to apply sequence numbers to IP access list entries simplifies access list changes. Prior to the IP Access List Entry Sequence Numbering feature, there was no way to specify the position of an entry within an access list. If a user wanted to insert an entry (statement) in the middle of an existing list, all of the entries after the desired position had to be removed, then the new entry was added, and then all the removed entries had to be reentered. This method was cumbersome and error prone.

This feature allows users to add sequence numbers to access list entries and resequence them. When a user adds a new entry, the user chooses the sequence number so that it is in a desired position in the access list. If necessary, entries currently in the access list can be resequenced to create room to insert the new entry.

**Sequence Numbering Behavior**

- For backward compatibility with previous releases, if entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

  Exceeded maximum sequence number.

- If the user enters an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.
• If the user enters an entry that matches an already existing entry (except for the sequence number), then no changes are made.

• If the user enters a sequence number that is already present, the following error message is generated:

    Duplicate sequence number.

• If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.

• Distributed support is provided so that the sequence numbers of entries in the Route Processor (RP) and line card are in synchronization at all times.

• Sequence numbers are not nvgened. That is, the sequence numbers themselves are not saved. In the event that the system is reloaded, the configured sequence numbers revert to the default sequence starting number and increment. The function is provided for backward compatibility with software releases that do not support sequence numbering.

• This feature works with named and numbered, standard and extended IP access lists.

Including comments in ACLs

You can use the **remark** keyword to include comments (remarks) about entries in any IP standard or extended ACL. The remarks make the ACL easier for you to understand and scan. Each remark line is limited to 100 characters.

The remark can go before or after a permit or deny statement. You should be consistent about where you put the remark so that it is clear which remark describes which permit or deny statement. For example, it would be confusing to have some remarks before the associated permit or deny statements and some remarks after the associated statements.

To include a comment for IP numbered standard or extended ACLs, use the **access-list access-list number remark remark** global configuration command. To remove the remark, use the **no** form of this command.

The following is an example of a remark that describes function of the subsequent deny statement:

```
ip access-list extended telnetting
    remark Do not allow host1 subnet to telnet out
deny tcp host 172.16.2.88 any eq telnet
```

Hardware and Software Treatment of IP ACLs

ACL processing is performed at the hardware side. If the hardware reaches its capacity to store ACL configurations, the packets are sent to the CPU, where ACL is processed at the software side. When sent for software ACL, the data packets are not sent at the line rate; instead, they are sent at a very low rate via rate limiting.

---

**Note**

If an ACL configuration cannot be implemented in hardware due to an out-of-resource condition on a switch, then only the traffic in that VLAN arriving on that switch is affected. Software forwarding of packets might adversely impact the performance of the switch, depending on the number of CPU cycles that this consumes.
When traffic flows are both logged and forwarded, forwarding is done by hardware, but logging must be done by software. Because of the difference in packet handling capacity between hardware and software, if the sum of all flows being logged (both permitted flows and denied flows) is of great enough bandwidth, not all of the packets that are forwarded can be logged.

When you enter the `show ip access-lists` privileged EXEC command, the match count displayed does not account for packets that are access controlled in hardware. ACLs function as follows:

- The hardware controls permit and deny actions of standard and extended ACLs (input and output) for security access control.
- If `log` has not been specified, the flows that match a `deny` statement in a security ACL are dropped by the hardware if `ip unreachables` is disabled. The flows matching a `permit` statement are switched in hardware.
- Adding the `log` keyword to an ACE in an ACL causes a copy of the packet to be sent to the CPU for logging only. If the ACE is a `permit` statement, the packet is still switched in hardware.

**Time Ranges for ACLs**

You can selectively apply extended ACLs based on the time of day and the week by using the `time-range` global configuration command. First, define a time-range name and set the times and the dates or the days of the week in the time range. Then enter the time-range name when applying an ACL to set restrictions to the access list. You can use the time range to define when the permit or deny statements in the ACL are in effect, for example, during a specified time period or on specified days of the week. The `time-range` keyword and argument are referenced in the named and numbered extended ACL task tables.

These are some benefits of using time ranges:

- You have more control over permitting or denying a user access to resources, such as an application (identified by an IP address/mask pair and a port number).
- You can control logging messages. ACL entries can be set to log traffic only at certain times of the day. Therefore, you can simply deny access without needing to analyze many logs generated during peak hours.

Time-based access lists trigger CPU activity because the new configuration of the access list must be merged with other features and the combined configuration loaded into the hardware memory. For this reason, you should be careful not to have several access lists configured to take effect in close succession (within a small number of minutes of each other.)

**Note**

The time range relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock.

**IPv4 ACL Interface Considerations**

When you apply the `ip access-group` interface configuration command to a Layer 3 interface (an SVI, a Layer 3 EtherChannel, or a routed port), the interface must have been configured with an IP address. Layer 3 access groups filter packets that are routed or are received by Layer 3 processes on the CPU. They do not affect packets bridged within a VLAN.
For inbound ACLs, after receiving a packet, the switch checks the packet against the ACL. If the ACL permits the packet, the switch continues to process the packet. If the ACL rejects the packet, the switch discards the packet.

For outbound ACLs, after receiving and routing a packet to a controlled interface, the switch checks the packet against the ACL. If the ACL permits the packet, the switch sends the packet. If the ACL rejects the packet, the switch discards the packet.

When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied to the interface and permits all packets. Remember this behavior if you use undefined ACLs for network security.

Apply an Access Control List to an Interface

With some protocols, you can apply up to two access lists to an interface: one inbound access list and one outbound access list. With other protocols, you apply only one access list that checks both inbound and outbound packets.

If the access list is inbound, when a device receives a packet, Cisco software checks the access list’s criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software discards the packet.

If the access list is outbound, after receiving and routing a packet to the outbound interface, Cisco software checks the access list’s criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is denied, the software discards the packet.

Access lists that are applied to interfaces on a device do not filter traffic that originates from that device.

Figure 53: Topology for Applying Access Control Lists

The figure above shows that Device 2 is a bypass device that is connected to Device 1 and Device 3. An outbound access list is applied to Gigabit Ethernet interface 0/0/0 on Device 1. When you ping Device 3 from Device 1, the access list does not check for packets going outbound because the traffic is locally generated. The access list check is bypassed for locally generated packets, which are always outbound.

By default, an access list that is applied to an outbound interface for matching locally generated traffic will bypass the outbound access list check; but transit traffic is subjected to the outbound access list check.

The behavior described above applies to all single-CPU platforms that run Cisco software.
The switch software can provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the ACL causes an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the `logging console` commands controlling the syslog messages.

**Note**
ACL logging is only supported for RACL.

**Note**
Because routing is done in hardware and logging is done in software, if a large number of packets match a permit or deny ACE containing a `log` keyword, the software might not be able to match the hardware processing rate, and not all packets will be logged.

The first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

**Note**
The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

### How to Configure ACLs

#### Configuring IPv4 ACLs

These are the steps to use IP ACLs on the switch:

**SUMMARY STEPS**

1. Create an ACL by specifying an access list number or name and the access conditions.
2. Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create an ACL by specifying an access list number or name and the access conditions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.</td>
</tr>
</tbody>
</table>
Creating a Numbered Standard ACL

Follow these steps to create a numbered standard ACL:

SUMMARY STEPS

1. enable
2. configure terminal
3. access-list access-list-number {deny | permit} source source-wildcard [log]
4. end
5. show running-config
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> access-list access-list-number {deny</td>
<td>permit} source source-wildcard [log]</td>
</tr>
<tr>
<td>Example: Switch(config)# access-list 2 deny your_host</td>
<td></td>
</tr>
<tr>
<td>The access-list-number is a decimal number from 1 to 99 or 1300 to 1999. Enter deny or permit to specify whether to deny or permit access if conditions are matched.</td>
<td></td>
</tr>
<tr>
<td>The source is the source address of the network or host from which the packet is being sent specified as:</td>
<td></td>
</tr>
<tr>
<td>• The 32-bit quantity in dotted-decimal format.</td>
<td></td>
</tr>
<tr>
<td>• The keyword any as an abbreviation for source and source-wildcard of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard.</td>
<td></td>
</tr>
<tr>
<td>• The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0.</td>
<td></td>
</tr>
<tr>
<td>(Optional) The source-wildcard applies wildcard bits to the source.</td>
<td></td>
</tr>
</tbody>
</table>
Creating a Numbered Extended ACL

Follow these steps to create a numbered extended ACL:

**SUMMARY STEPS**

1. configure terminal
2. access-list access-list-number \{deny | permit\} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp]
3. access-list access-list-number \{deny | permit\} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp] [flag]
4. access-list access-list-number \{deny | permit\} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp]
5. access-list access-list-number \{deny | permit\} icmp source source-wildcard destination destination-wildcard [icmp-type | [icmp-type icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]
6. access-list access-list-number \{deny | permit\} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp]
7. end
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`access-list access-list-number {deny</td>
<td>permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log</code></td>
<td></td>
</tr>
</tbody>
</table>

The `access-list-number` is a decimal number from 100 to 199 or 2000 to 2699.

Enter `deny` or `permit` to specify whether to deny or permit the packet if conditions are matched.

For `protocol`, enter the name or number of an IP protocol: `ahp, eigrp, esp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, tcp, or udp`, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword `ip`.

**Note** This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see the following steps.

The `source` is the number of the network or host from which the packet is sent.

The `source-wildcard` applies wildcard bits to the source.

The `destination` is the network or host number to which the packet is sent.

The `destination-wildcard` applies wildcard bits to the destination.

Source, source-wildcard, destination, and destination-wildcard can be specified as:

- The 32-bit quantity in dotted-decimal format.
- The keyword `any` for 0.0.0.0 255.255.255.255 (any host).
- The keyword `host` for a single host 0.0.0.0.

The other keywords are optional and have these meanings:

- `precedence`—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: `routine` (0), `priority` (1), `immediate` (2), `flash` (3), `flash-override` (4), `critical` (5), `internet` (6), `network` (7).
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• fragments—Enter to check non-initial fragments.</td>
<td></td>
</tr>
<tr>
<td>• tos—Enter to match by type of service level, specified by a number from 0 to 15 or a name: normal (0), max-reliability (2), max-throughput (4), min-delay (8).</td>
<td></td>
</tr>
<tr>
<td>• log—Enter to create an informational logging message to be sent to the console about the packet that matches the entry or log-input to include the input interface in the log entry.</td>
<td></td>
</tr>
<tr>
<td>• time-range—Specify the time-range name.</td>
<td></td>
</tr>
<tr>
<td>• dscp—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** If you enter a dscp value, you cannot enter tos or precedence. You can enter both a tos and a precedence value with no dscp.

### Step 3

```plaintext
access-list access-list-number {deny | permit} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp] [flag]
```

**Example:**

```plaintext
Switch(config)# access-list 101 permit tcp any any eq 500
```

Defines an extended TCP access list and the access conditions.

The parameters are the same as those described for an extended IPv4 ACL, with these exceptions:

(Optional) Enter an operator and port to compare source (if positioned after source source-wildcard) or destination (if positioned after destination destination-wildcard) port. Possible operators include eq (equal), gt (greater than), lt (less than), neq (not equal), and range (inclusive range). Operators require a port number (range requires two port numbers separated by a space).

Enter the port number as a decimal number (from 0 to 65535) or the name of a TCP port. Use only TCP port numbers or names when filtering TCP.

The other optional keywords have these meanings:

- **established**—Enter to match an established connection. This has the same function as matching on the ack or rst flag.

- **flag**—Enter one of these flags to match by the specified TCP header bits: ack (acknowledge), fin (finish), psh (push), rst (reset), syn (synchronize), or urg (urgent).

### Step 4

```plaintext
access-list access-list-number {deny | permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence]
```

(Optional) Defines an extended UDP access list and the access conditions.
### Command or Action

- `precedence`  
- `[tos tos]`  
- `[fragments]`  
- `[log [log-input]`  
- `[time-range time-range-name]`  
- `[dscp dscp]`

**Example:**

```
Switch(config)# access-list 101 permit udp any any eq 100
```

### Purpose

The UDP parameters are the same as those described for TCP except that the `[operator [port]]` port number or name must be a UDP port number or name, and the `flag` keyword is and `established` keywords are not valid for UDP.

### Step 5

**access-list access-list-number {deny | permit} icmp source source-wildcard destination destination-wildcard [icmp-type | [icmp-type icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]**

**Example:**

```
Switch(config)# access-list 101 permit icmp any any 200
```

### Purpose

Defines an extended ICMP access list and the access conditions.

The ICMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

- `icmp-type`—Enter to filter by ICMP message type, a number from 0 to 255.
- `icmp-code`—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.
- `icmp-message`—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name.

### Step 6

**access-list access-list-number {deny | permit} igmp source source-wildcard destination destination-wildcard [igmp-type [precedence precedence] [tos tos] [fragments] [log [log-input] [time-range time-range-name] [dscp dscp]**

**Example:**

```
Switch(config)# access-list 101 permit igmp any any 14
```

### Purpose

(Optional) Defines an extended IGMP access list and the access conditions.

The IGMP parameters are the same as those described for most IP protocols in an extended IPv4 ACL, with this optional parameter.

- `igmp-type`—To match IGMP message type, enter a number from 0 to 15, or enter the message name: `dvmrp`, `host-query`, `host-report`, `pim`, or `trace`.

### Step 7

**end**

**Example:**

```
Switch(config)# end
```

### Purpose

Returns to privileged EXEC mode.

---

**Creating Named Standard ACLs**

Follow these steps to create a standard ACL using names:

**SUMMARY STEPS**

1. `enable`
2. configure terminal
3. ip access-list standard name
4. Use one of the following:
   • deny {source [source-wildcard] | host source | any} [log]
   • permit {source [source-wildcard] | host source | any} [log]
5. end
6. show running-config
7. copy running-config startup-config

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip access-list standard name</td>
<td>Defines a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip access-list standard 20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> Use one of the following:</td>
<td></td>
</tr>
<tr>
<td>• deny {source [source-wildcard]</td>
<td>host source</td>
</tr>
<tr>
<td>• permit {source [source-wildcard]</td>
<td>host source</td>
</tr>
<tr>
<td>Example: Switch(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</td>
<td></td>
</tr>
<tr>
<td>or Switch(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>
### Creating Extended Named ACLs

Follow these steps to create an extended ACL using names:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip access-list extended name`
4. `{deny | permit} protocol [source [source-wildcard] | host source | any] {destination [destination-wildcard] | host destination | any} [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 3

**ip access-list extended** *name*

**Example:**

Switch(config)# ip access-list extended 150

**Purpose:** Defines an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199.

**Example:**

Step 3

#### Step 4

```plaintext
\{deny | permit\} protocol \{source [source-wildcard] | host source | any\} \{destination [destination-wildcard] | host destination | any\} \{precedence precedence\} [tos tos] [established] [log] [time-range time-range-name]
```

**Example:**

Switch(config-ext-nacl)# permit 0 any any

**Purpose:** In access-list configuration mode, specify the conditions allowed or denied. Use the log keyword to get access list logging messages, including violations.

- **host source**—A source and source wildcard of source 0.0.0.0.
- **host destination**—A destination and destination wildcard of destination 0.0.0.0.
- **any**—A source and source wildcard or destination and destination wildcard of 0.0.0.0 255.255.255.255.

#### Step 5

**end**

**Example:**

Switch(config-ext-nacl)# end

**Purpose:** Returns to privileged EXEC mode.

#### Step 6

**show running-config**

**Example:**

Switch# show running-config

**Purpose:** Verifies your entries.

#### Step 7

**copy running-config startup-config**

**Example:**

Switch# copy running-config startup-config

**Purpose:** (Optional) Saves your entries in the configuration file.

---

When you are creating extended ACLs, remember that, by default, the end of the ACL contains an implicit deny statement for everything if it did not find a match before reaching the end. For standard ACLs, if you omit the mask from an associated IP host address access list specification, 0.0.0.0 is assumed to be the mask.

After you create an ACL, any additions are placed at the end of the list. You cannot selectively add ACL entries to a specific ACL. However, you can use no permit and no deny access-list configuration mode commands to remove entries from a named ACL.

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.
What to do next

After creating a named ACL, you can apply it to interfaces or to VLANs.

Sequencing Access-List Entries and Revising the Access List

This task shows how to assign sequence numbers to entries in a named IP access list and how to add or delete an entry to or from an access list. When completing this task, keep the following points in mind:

- Resequencing the access list entries is optional. The resequencing step in this task is shown as required because that is one purpose of this feature and this task demonstrates that functionality.
- In the following procedure, the `permit` command is shown in Step 5 and the `deny` command is shown in Step 6. However, that order can be reversed. Use the order that suits the need of your configuration.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip access-list resequence access-list-name starting-sequence-number increment`
4. `ip access-list {standard extended} access-list-name`
5. Do one of the following:
   - `sequence-number permit source source-wildcard`
   - `sequence-number permit protocol source-source-wildcard destination destination-wildcard [precedence precedence][tos tos] [log] [time-range time-range-name] [fragments]`
6. Do one of the following:
   - `sequence-number deny source source-wildcard`
   - `sequence-number deny protocol source-source-wildcard destination destination-wildcard [precedence precedence][tos tos] [log] [time-range time-range-name] [fragments]`
7. Do one of the following:
   - `sequence-number permit source source-wildcard`
   - `sequence-number permit protocol source-source-wildcard destination destination-wildcard [precedence precedence][tos tos] [log] [time-range time-range-name] [fragments]`
8. Do one of the following:
   - `sequence-number deny source source-wildcard`
   - `sequence-number deny protocol source-source-wildcard destination destination-wildcard [precedence precedence][tos tos] [log] [time-range time-range-name] [fragments]`
9. Repeat Step 5 and/or Step 6 to add sequence number statements, as applicable.
10. `end`
11. `show ip access-lists access-list-name`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip access-list resequence access-list-name starting-sequence-number increment</td>
<td>Resequences the specified IP access list using the starting sequence number and the increment of sequence numbers.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip access-list resequence kmd1 100 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip access-list {standard</td>
<td>extended} access-list-name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip access-list standard kmd1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> Do one of the following:</td>
<td>Specifies a permit statement in named IP access list mode.</td>
</tr>
<tr>
<td>• sequence-number permit source source-wildcard</td>
<td></td>
</tr>
<tr>
<td>• sequence-number permit protocol source source-wildcard destination destination-wildcard [precedence precedence][tos tos][log][time-range time-range-name] [fragments]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-std-nacl)# 105 permit 10.5.5.5 0.0.0.0 255</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> Do one of the following:</td>
<td>(Optional) Specifies a deny statement in named IP access list mode.</td>
</tr>
<tr>
<td>• sequence-number deny source source-wildcard</td>
<td></td>
</tr>
<tr>
<td>• sequence-number deny protocol source source-wildcard destination destination-wildcard [precedence precedence][tos tos][log][time-range time-range-name] [fragments]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)*
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-std-nacl)# 105 deny 10.6.6.7 0.0.0 255</td>
<td>the prompt for this step would be Device(config-ext-nacl) and you would use the extended deny command syntax.</td>
</tr>
</tbody>
</table>

#### Step 7

Do one of the following:

- `sequence-number permit source source-wildcard`
- `sequence-number permit protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]`

**Example:**

Device(config-ext-nacl)# 150 permit tcp any any log

#### Step 8

Do one of the following:

- `sequence-number deny source source-wildcard`
- `sequence-number deny protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]`

**Example:**

Device(config-ext-nacl)# 150 deny tcp any any log

#### Step 9

Repeat Step 5 and/or Step 6 to add sequence number statements, as applicable.

Allows you to revise the access list.

#### Step 10

`end`

**Example:**

Device(config-std-nacl)# end

#### Step 11

`show ip access-lists access-list-name`

**Example:**

Device# show ip access-lists kmd1

### Examples

Review the output of the `show ip access-lists` command to see that the access list includes the new entries:

Device# show ip access-lists kmd1

---

*Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)*
Standard IP access list kmd1
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.0, wildcard bits 0.0.0.255
115 permit 10.0.0.0, wildcard bits 0.0.0.255
130 permit 10.5.5.0, wildcard bits 0.0.0.255
145 permit 10.0.0.0, wildcard bits 0.0.0.255

Configuring Commented IP ACL Entries

Either use a named or numbered access list configuration. You must apply the access list to an interface or terminal line after the access list is created for the configuration to work.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip access-list {standard | extended} {name | number}
4. remark remark
5. deny protocol host host-address any eq port
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        |       |
| configure terminal| Enters global configuration mode. |
| Example:          |         |
| Device# configure terminal | |

| **Step 3**        |       |
| ip access-list {standard | extended} {name | number} | Identifies the access list by a name or number and enters extended named access list configuration mode. |
| Example:          |         |
| Device(config)# ip access-list extended telnetting | |

| **Step 4**        |       |
| remark remark      | Adds a remark for an entry in a named IP access list. |
| Example:          | • The remark indicates the purpose of the permit or deny statement. |
| Device(config-ext-nacl)# remark Do not allow host1 subnet to telnet out | |

| **Step 5**        |       |
| deny protocol host host-address any eq port | Sets conditions in a named IP access list that denies packets. |
| Example:          |         |
| Device(config-ext-nacl)# deny tcp host 172.16.2.88 any eq telnet | |
Configuring Time Ranges for ACLs

Follow these steps to configure a time-range parameter for an ACL:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. time-range time-range-name
4. Use one of the following:
   - **absolute** [start time date] [end time date]
   - **periodic** day-of-the-week hh:mm to [day-of-the-week] hh:mm
   - **periodic** {weekdays | weekend | daily} hh:mm to hh:mm
5. end
6. show running-config
7. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>time-range time-range-name</td>
<td>Assigns a meaningful name (for example, workhours) to the time range to be created, and enter time-range configuration mode. The name cannot contain a space or quotation mark and must begin with a letter.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# time-range workhours</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Use one of the following:</td>
<td>Specifies when the function it will be applied to is operational.</td>
</tr>
<tr>
<td></td>
<td>• <strong>absolute</strong> [start time date] [end time date]</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| • **periodic** day-of-the-week hh:mm to [day-of-the-week] hh:mm  
• **periodic** {weekdays | weekend | daily} hh:mm to hh:mm | • You can use only one **absolute** statement in the time range. If you configure more than one absolute statement, only the one configured last is executed.  
• You can enter multiple **periodic** statements. For example, you could configure different hours for weekdays and weekends.  
See the example configurations. |

**Example:**

Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006

or

Switch(config-time-range)# periodic weekdays 8:00 to 12:00

**Step 5**

**end**

**Example:**

Switch(config)# end

**Step 6**

**show running-config**

**Example:**

Switch# show running-config

**Step 7**

**copy running-config startup-config**

**Example:**

Switch# copy running-config startup-config

**What to do next**

Repeat the steps if you have multiple items that you want in effect at different times.

**Applying an IPv4 ACL to a Terminal Line**

You can use numbered ACLs to control access to one or more terminal lines. You cannot apply named ACLs to lines. You must set identical restrictions on all the virtual terminal lines because a user can attempt to connect to any of them.

Follow these steps to restrict incoming and outgoing connections between a virtual terminal line and the addresses in an ACL:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. line [console | vty] line-number
4. access-class access-list-number {in | out}
5. end
6. show running-config
7. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch(config)# enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> line [console</td>
<td>vty] line-number</td>
</tr>
<tr>
<td>Example: Switch(config)# line console 0</td>
<td></td>
</tr>
<tr>
<td>• console—Specifies the console terminal line. The console port is DCE.</td>
<td></td>
</tr>
<tr>
<td>• vty—Specifies a virtual terminal for remote console access.</td>
<td></td>
</tr>
<tr>
<td>The line-number is the first line number in a contiguous group that you want to configure when the line type is specified. The range is from 0 to 16.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> access-class access-list-number {in</td>
<td>out}</td>
</tr>
<tr>
<td>Example: Switch(config-line)# access-class 10 in</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-line)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

---

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
### Applying an IPv4 ACL to an Interface

This section describes how to apply IPv4 ACLs to network interfaces. Beginning in privileged EXEC mode, follow these steps to control access to an interface:

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `ip access-group {access-list-number | name} {in | out}`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **configure terminal**
| Example: | Switch# configure terminal |
| **Step 2** | **interface interface-id**
| Example: | Switch(config)# interface gigabitethernet 0/1 |
| **Step 3** | **ip access-group {access-list-number | name} {in | out}**
<p>| Example: | Switch(config-if)# ip access-group 2 in |</p>
<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

## Monitoring IPv4 ACLs

You can monitor IPv4 ACLs by displaying the ACLs that are configured on the switch, and displaying the ACLs that have been applied to interfaces and VLANs.

When you use the `ip access-group` interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in this table to display this information.

### Table 81: Commands for Displaying Access Lists and Access Groups

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show access-lists [number</td>
<td>name]`</td>
</tr>
<tr>
<td>`show ip access-lists [number</td>
<td>name]`</td>
</tr>
<tr>
<td><code>show ip interface interface-id</code></td>
<td>Displays detailed configuration and status of an interface. If IP is enabled on the interface and ACLs have been applied by using the <code>ip access-group</code> interface configuration command, the access groups are included in the display.</td>
</tr>
<tr>
<td><code>show running-config [interface interface-id]</code></td>
<td>Displays the contents of the configuration file for the switch or the specified interface, including all configured MAC and IP access lists and which access groups are applied to an interface.</td>
</tr>
</tbody>
</table>
### Configuration Examples for ACLs

#### ACLs in a Small Networked Office

**Figure 54: Using Router ACLs to Control Traffic**

This shows a small networked office environment with routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing confidential payroll data. All users can access Server A, but Server B has restricted access.

Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.

#### Example: Numbered ACLs

In this example, network 10.0.0.0 is a Class A network whose second octet specifies a subnet; that is, its subnet mask is 255.255.0.0. The third and fourth octets of a network 10.0.0.0 address specify a particular host. Using access list 2, the switch accepts one address on subnet 48 and reject all others on that subnet. The last...
line of the list shows that the switch accepts addresses on all other network 10.0.0.0 subnets. The ACL is applied to packets entering a port.

Switch(config)# access-list 2 permit 10.48.0.3
Switch(config)# access-list 2 deny 10.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 10.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip access-group 2 in

Examples: Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip access-group 102 in

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Outbound packets have the port numbers reversed. Because the secure system of the network always accepts mail connections on port 25, the incoming and outgoing services are separately controlled. The ACL must be configured as an input ACL on the outbound interface and an output ACL on the inbound interface.

Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip access-group 102 in

In this example, the network is a Class B network with the address 128.88.0.0, and the mail host address is 128.88.1.2. The **ACK** or **RST** keywords are used to match ACK or RST bits set, which show that the packet belongs to an existing connection.

Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 RST
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip access-group 102 in

In this example, the network is a Class B network with the address 128.88.0.0, and the mail host address is 128.88.1.2. The **established** keyword is used only for the TCP to show an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which show that the packet belongs to an existing connection.
connection. Gigabit Ethernet interface 1 on stack member 1 is the interface that connects the router to the Internet.

Examples: Named ACLs

Creating named standard and extended ACLs

This example creates a standard ACL named `internet_filter` and an extended ACL named `marketing_group`. The `internet_filter` ACL allows all traffic from the source address 1.2.3.4.

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

The `marketing_group` ACL allows any TCP Telnet traffic to the destination address and wildcard 171.69.0.0 0.0.255.255 and denies any other TCP traffic. It permits ICMP traffic, denies UDP traffic from any source to the destination address range 171.69.0.0 through 179.69.255.255 with a destination port less than 1024, denies any other IP traffic, and provides a log of the result.

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

Deleting individual ACEs from named ACLs

This example shows how you can delete individual ACEs from the named access list `border-list`:

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

Example Resequencing Entries in an Access List

The following example shows an access list before and after resequencing. The starting value is 1, and increment value is 2. The subsequent entries are ordered based on the increment values that users provide, and the range is from 1 to 2147483647.

When an entry with no sequence number is entered, by default it has a sequence number of 10 more than the last entry in the access list.

```
Router# show access-list carls
Extended IP access list carls
   10 permit ip host 10.3.3.3 host 172.16.5.34
   20 permit icmp any any
   30 permit tcp any host 10.3.3.3
   40 permit ip host 10.4.4.4 any
   50 Dynamic test permit ip any any
   60 permit ip host 172.16.2.2 host 10.3.3.12
```
Example Adding an Entry with a Sequence Number

In the following example, an new entry (sequence number 15) is added to an access list:

```
Router# show ip access-list
Standard IP access list tryon
  2 permit 10.4.4.2, wildcard bits 0.0.255.255
  5 permit 10.0.0.44, wildcard bits 0.0.0.255
 10 permit 10.0.0.1, wildcard bits 0.0.0.255
 20 permit 10.0.0.2, wildcard bits 0.0.0.255
Router(config)# ip access-list standard tryon
Router(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255
Router# show ip access-list
Standard IP access list tryon
  2 permit 10.4.0.0, wildcard bits 0.0.255.255
  5 permit 10.0.0.0, wildcard bits 0.0.0.255
 10 permit 10.0.0.0, wildcard bits 0.0.0.255
 15 permit 10.5.5.0, wildcard bits 0.0.0.255
 20 permit 10.0.0.0, wildcard bits 0.0.0.255
```

Example Adding an Entry with No Sequence Number

The following example shows how an entry with no specified sequence number is added to the end of an access list. When an entry is added without a sequence number, it is automatically given a sequence number that puts it at the end of the access list. Because the default increment is 10, the entry will have a sequence number 10 higher than the last entry in the existing access list.

```
Router(config)# ip access-list standard resources
Router(config-std-nacl)#  permit 10.1.1.1 0.0.0.255
Router(config-std-nacl)#  permit 10.2.2.2 0.0.0.255
Router(config-std-nacl)#  permit 10.3.3.3 0.0.0.255
Router# show access-list
Standard IP access list resources
 10 permit 10.1.1.1, wildcard bits 0.0.0.255
 20 permit 10.2.2.2, wildcard bits 0.0.0.255
 30 permit 10.3.3.3, wildcard bits 0.0.0.255
Router(config)# ip access-list standard resources
Router(config-std-nacl)#  permit 10.4.4.4 0.0.0.255
```
Examples: Configuring Commented IP ACL Entries

In this example of a numbered ACL, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13

In this example of a numbered ACL, the Winter and Smith workstations are not allowed to browse the web:

Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www

In this example of a named ACL, the Jones subnet is not allowed access:

Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255

In this example of a named ACL, the Jones subnet is not allowed to use outbound Telnet:

Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet

Examples: Using Time Ranges with ACLs

This example shows how to verify after you configure time ranges for workhours and to configure January 1, 2006, as a company holiday.

Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
  absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
  periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00

To apply a time range, enter the time-range name in an extended ACL that can implement time ranges. This example shows how to create and verify extended access list 188 that denies TCP traffic from any source to any destination during the defined holiday times and permits all TCP traffic during work hours.
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
  10 deny tcp any any time-range new_year_day_2006 (inactive)
  20 permit tcp any any time-range workhours (inactive)

This example uses named ACLs to permit and deny the same traffic.

Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
  10 permit ip any
Extended IP access list deny_access
  10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
  10 permit tcp any any time-range workhours (inactive)

Examples: Time Range Applied to an IP ACL

This example denies HTTP traffic on IP on Monday through Friday between the hours of 8:00 a.m. and 6:00 p.m. (18:00). The example allows UDP traffic only on Saturday and Sunday from noon to 8:00 p.m. (20:00).

Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
! Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
! Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
! Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet 0/1 interface gigabitethernet2/0/1
Switch(config-if)# ip access-group strict in

Examples: ACL Logging

Two variations of logging are supported on router ACLs. The log keyword sends an informational logging message to the console about the packet that matches the entry; the log-input keyword includes the input interface in the log entry.

In this example, standard named access list stan1 denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the log keyword.

Switch(config)# ip access-list standard stan1
Examples: ACL Logging

Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
Console logging: level debugging, 37 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 37 messages logged
File logging: disabled
Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):
00:00:48: NTP: authentication delay calculation problems
<output truncated>
00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet

This example is a named extended access list ext1 that permits ICMP packets from any source to 10.1.1.0 0.0.0.255 and denies all UDP packets.

Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# ip access-group ext1 in

This is an example of a log for an extended ACL:

01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1 packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7 packets
01:26:12:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1 packet
01:31:33:%SEC-6-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8 packets

Note that all logging entries for IP ACLs start with %SEC-6-IPACCESSLOG with minor variations in format depending on the kind of ACL and the access entry that has been matched.

This is an example of an output message when the log-input keyword is entered:

00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet

A log message for the same sort of packet using the log keyword does not include the input interface information:

00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0), 1 packet
packet

Examples: Troubleshooting ACLs

If this ACL manager message appears and [chars] is the access-list name,

ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]

The switch has insufficient resources to create a hardware representation of the ACL. The resources include hardware memory and label space but not CPU memory. A lack of available logical operation units or specialized hardware resources causes this problem. Logical operation units are needed for a TCP flag match or a test other than `eq (ne, gt, lt, or range)` on TCP, UDP, or SCTP port numbers.

Use one of these workarounds:

- Modify the ACL configuration to use fewer resources.
- Rename the ACL with a name or number that alphanumerically precedes the ACL names or numbers.

To determine the specialized hardware resources, enter the `show platform layer4 acl` map privileged EXEC command. If the switch does not have available resources, the output shows that index 0 to index 15 are not available.

For more information about configuring ACLs with insufficient resources, see CSCsq63926 in the Bug Toolkit.

For example, if you apply this ACL to an interface:

```plaintext
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

And if this message appears:

ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]

The flag-related operators are not available. To avoid this issue,

- Move the fourth ACE before the first ACE by using `ip access-list resequence` global configuration command:

```plaintext
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

or

- Rename the ACL with a name or number that alphanumerically precedes the other ACLs (for example, rename ACL 79 to ACL 1).
You can now apply the first ACE in the ACL to the interface. The switch allocates the ACE to available mapping bits in the Opselect index and then allocates flag-related operators to use the same bits in the hardware memory.

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Command List, All Releases</em></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature Information for IPv4 Access Control Lists

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>IPv4 Access Control Lists perform packet filtering to control which packets move through the network and where. Such control provides security by helping to limit network traffic, restrict the access of users and devices to the network, and prevent traffic from leaving a network. This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Feature Information</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco IOS 15.2(2)E</td>
<td>The Named ACL Support for Noncontiguous Ports on an Access Control Entry feature allows you to specify noncontiguous ports in a single access control entry, which greatly reduces the number of entries required in an access control list when several entries have the same source address, destination address, and protocol, but differ only in the ports.</td>
</tr>
<tr>
<td>Cisco IOS 15.2(2)E</td>
<td>The IP Access List Entry Sequence Numbering feature helps users to apply sequence numbers to permit or deny statements and also reorder, add, or remove such statements from a named IP access list. This feature makes revising IP access lists much easier. Prior to this feature, users could add access list entries to the end of an access list only; therefore needing to add statements anywhere except the end required reconfiguring the access list entirely. The following commands were introduced or modified: <code>deny (IP)</code>, <code>ip access-list resequence deny (IP)</code>, <code>permit (IP)</code>.</td>
</tr>
</tbody>
</table>
IPv6 Access Control Lists

Access lists determine what traffic is blocked and what traffic is forwarded at device interfaces and allow filtering of traffic based on source and destination addresses, and inbound and outbound traffic to a specific interface. Standard IPv6 ACL functionality was extended to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control. Standard IPv6 ACL functionality was extended to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control.

This module describes how to configure IPv6 traffic filtering and to control access to virtual terminal lines.

• Finding Feature Information, on page 783
• Restrictions for IPv6 ACLs, on page 783
• Information About Configuring IPv6 ACLs, on page 784
• How to Configure IPv6 ACLs, on page 786
• Configuration Examples for IPv6 ACLs, on page 794
• Additional References, on page 796
• Feature Information for IPv6 Access Control Lists, on page 796

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPv6 ACLs

With IPv4, you can configure standard and extended numbered IP ACLs, named IP ACLs, and MAC ACLs. IPv6 supports only named ACLs.

The switch supports most Cisco IOS-supported IPv6 ACLs with some exceptions:
• The switch does not support matching on these keywords: **flowlabel**, **routing header**, and **undetermined-transport**.

• The switch does not support reflexive ACLs (the **reflect** keyword).

• This release supports only port ACLs and router ACLs for IPv6; it does not support VLAN ACLs (VLAN maps).

• The switch does not apply MAC-based ACLs on IPv6 frames.

• You cannot apply IPv6 port ACLs to Layer 2 EtherChannels.

• When configuring an ACL, there is no restriction on keywords entered in the ACL, regardless of whether or not they are supported on the platform. When you apply the ACL to an interface that requires hardware forwarding (physical ports or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.

• If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

**IPv6 ACLs on the switch have these characteristics:**

• The same statistics supported in IPv4 are supported for IPv6 ACLs.

• If the switch runs out of hardware space, the packets associated with the ACL are dropped on the interface.

• Routed or bridged packets with hop-by-hop options have IPv6 ACLs applied in software.

• The switch supports IPv6 address-matching for a full range of prefix-lengths.

---

**Information About Configuring IPv6 ACLs**

You can filter IP version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similarly to the way that you create and apply IP version 4 (IPv4) named ACLs.

**ACL Overview**

Packet filtering can help limit network traffic and restrict network use by certain users or devices. ACLs filter traffic as it passes through a router or switch and permit or deny packets crossing specified interfaces or VLANs. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. One by one, it tests packets against the conditions in an access list. The first match decides whether the switch accepts or rejects the packets. Because the switch stops testing after the first match, the order of conditions in the list is critical. If no conditions match, the switch rejects the packet. If there are no restrictions, the switch forwards the packet; otherwise, the switch drops the packet. The switch can use ACLs on all packets it forwards, including packets bridged within a VLAN.

You configure access lists on a router or Layer 3 switch to provide basic security for your network. If you do not configure ACLs, all packets passing through the switch could be allowed onto all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both.
IPv6 ACLs Overview

You can filter IP Version 6 (IPv6) traffic by creating IPv6 access control lists (ACLs) and applying them to interfaces similar to how you create and apply IP Version 4 (IPv4) named ACLs.

The switch does not support VLAN ACLs (VLAN maps) for IPv6 traffic.

You can apply both IPv4 and IPv6 ACLs to an interface.

Interactions with Other Features and Switches

• If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.

• You can create both IPv4 and IPv6 ACLs on a switch, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

• You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.

• If the hardware memory is full, packets are dropped on the interface and an unload error message is logged.

Default Configuration for IPv6 ACLs

The default IPv6 ACL configuration is as follows:

Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100

Supported ACL Features

IPv6 ACLs on the switch have these characteristics:

• Fragmented frames (the fragments keyword as in IPv4) are supported.

• The same statistics supported in IPv4 are supported for IPv6 ACLs.

• If the switch runs out of TCAM space, packets associated with the ACL label are forwarded to the CPU, and the ACLs are applied in software.
IPv6 Port-Based Access Control List Support

The IPv6 PACL feature provides the ability to provide access control (permit or deny) on Layer 2 switch ports for IPv6 traffic. IPv6 PACLs are similar to IPv4 PACLs, which provide access control on Layer 2 switch ports for IPv4 traffic. They are supported only in the ingress direction and in hardware.

A PACL can filter ingress traffic on Layer 2 interfaces based on Layer 3 and Layer 4 header information or non-IP Layer 2 information.

ACLs and Traffic Forwarding

The IPv6 ACL Extensions for Hop by Hop Filtering feature allows you to control IPv6 traffic that might contain hop-by-hop extension headers. You can configure an access control list (ACL) to deny all hop-by-hop traffic or to selectively permit traffic based on protocol.

IPv6 access control lists (ACLs) determine what traffic is blocked and what traffic is forwarded at device interfaces. ACLs allow filtering based on source and destination addresses, inbound and outbound to a specific interface. Use the `ipv6 access-list` command to define an IPv6 ACL, and the `deny` and `permit` commands to configure its conditions.

The IPv6 ACL Extensions for Hop by Hop Filtering feature implements RFC 2460 to support traffic filtering in any upper-layer protocol type.

How to Configure IPv6 ACLs

Configuring IPv6 ACLs

To filter IPv6 traffic, you perform these steps:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ipv6 access-list list-name`
4. `{deny | permit} [protocol {source-ipv6-prefix/prefix-length|any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [fragments] [log] [log-input] [routing] [sequence value] [time-range name]`
5. `{deny | permit} [tcp | udp] [source-ipv6-prefix/prefix-length | any | host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address] [operator [port-number]] [ack | dscp value] [established] [fin] [log] [log-input] [neq | port | protocol] [psh] [range [port | protocol] | rst | [routing] [sequence value] [syn] [time-range name] [urg]`
6. `{deny | permit} [tcp | udp] [source-ipv6-prefix/prefix-length | any | host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address] [operator [port-number]] [dscp value] [log] [log-input] [neq | port | protocol] [range [port | protocol] | [routing] [sequence value] [time-range name] ]`
7. `{deny | permit} [icmp | ipv6] [source-ipv6-prefix/prefix-length | any | host source-ipv6-address] [operator [port-number]] [destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address] [operator [port-number]] [dscp value] [fragments] [log] [log-input] [neq | port | protocol] [range [port | protocol] | [routing] [sequence value] [time-range name] ]`

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ipv6 access-list list-name</td>
<td>Defines an IPv6 ACL name, and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# ipv6 access-list example_acl_list</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>deny</td>
<td>permit</td>
</tr>
<tr>
<td></td>
<td>source-ipv6-prefix/ prefix-length</td>
<td>any</td>
</tr>
<tr>
<td></td>
<td>destination-ipv6-prefix/ prefix-length</td>
<td>any</td>
</tr>
<tr>
<td></td>
<td>dscp value</td>
<td>[fragments]</td>
</tr>
<tr>
<td></td>
<td>udp, or an integer in the range 0 to 255 representing an IPv6 protocol number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The source-ipv6-prefix/ prefix-length or destination-ipv6-prefix/ prefix-length is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter any as an abbreviation for the IPv6 prefix ::/0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For host source-ipv6-address or destination-ipv6-address, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons.</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>• (Optional) For operator, specify an operand that compares the source or destination ports of the specified protocol. Operands are <strong>lt</strong> (less than), <strong>gt</strong> (greater than), <strong>eq</strong> (equal), <strong>neq</strong> (not equal), and <strong>range</strong>. If the operator follows the <code>source-ipv6-prefix/prefix-length</code> argument, it must match the source port. If the operator follows the <code>destination-ipv6-prefix/prefix-length</code> argument, it must match the destination port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (Optional) The <strong>port-number</strong> is a decimal number from 0 to 65535 or the name of a TCP or UDP port. You can use TCP port names only when filtering TCP. You can use UDP port names only when filtering UDP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <strong>dscp</strong> value to match a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <strong>fragments</strong> to check noninitial fragments. This keyword is visible only if the protocol is ipv6.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <strong>log</strong> to cause an logging message to be sent to the console about the packet that matches the entry. Enter <strong>log-input</strong> to include the input interface in the log entry. Logging is supported only for router ACLs.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <strong>routing</strong> to specify that IPv6 packets be routed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <strong>sequence value</strong> to specify the sequence number for the access list statement. The acceptable range is from 1 to 4,294,967,295.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• (Optional) Enter <strong>time-range name</strong> to specify the time range that applies to the deny or permit statement.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

```plaintext
{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port | protocol}] [psh] [range {port | protocol}] [rst] [routing] [sequence value] [syn] [time-range name] [urg]
```

(Optional) Define a TCP access list and the access conditions.

Enter **tcp** for Transmission Control Protocol. The parameters are the same as those described in Step 3a, with these additional optional parameters:

- **ack**—Acknowledgment bit set.
- **established**—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• fin—Finished bit set; no more data from sender.</td>
<td></td>
</tr>
<tr>
<td>• neq {port</td>
<td>protocol}—Matches only packets that are not on a given port number.</td>
</tr>
<tr>
<td>• psh—Push function bit set.</td>
<td></td>
</tr>
<tr>
<td>• range {port</td>
<td>protocol}—Matches only packets in the port number range.</td>
</tr>
<tr>
<td>• rst—Reset bit set.</td>
<td></td>
</tr>
<tr>
<td>• syn—Synchronize bit set.</td>
<td></td>
</tr>
<tr>
<td>• urg—Urgent pointer bit set.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 6

(Optional) Define a UDP access list and the access conditions.

Enter **udp** for the User Datagram Protocol. The UDP parameters are the same as those described for TCP, except that the [operator [port]] port number or name must be a UDP port number or name, and the established parameter is not valid for UDP.

### Step 7

(Optional) Define an ICMP access list and the access conditions.

Enter **icmp** for Internet Control Message Protocol. The ICMP parameters are the same as those described for most IP protocols in Step 1, with the addition of the ICMP message type and code parameters. These optional keywords have these meanings:

- **icmp-type**—Enter to filter by ICMP message type, a number from 0 to 255.
- **icmp-code**—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.
- **icmp-message**—Enter to filter ICMP packets by the ICMP message type name or the ICMP message type and code name. To see a list of ICMP message type names and code names, use the ? key or see command reference for this release.

### Step 8

Return to privileged EXEC mode.

### Step 9

Verify the access list configuration.

### Step 10

Verifies your entries.

**Example:**

```bash
Step 1:
(deny | permit) udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]]
{dscp value} [log] [log-input] [neq {port | protocol}] [range {port | protocol}] [routing] [sequence value] [time-range name]
Step 2:
(deny | permit) icmp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [operator [port-number]]
{icmp-type [icmp-code] | icmp-message} [dscp value] [log] [log-input] [routing] [sequence value] [time-range name]
Step 3:
end
Step 4:
show ipv6 access-list
Step 5:
show running-config
```
### Attaching an IPv6 ACL to an Interface

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces. You can also apply ACLs only to inbound management traffic on Layer 3 interfaces.

Follow these steps to control access to an interface:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `no switchport`
5. `ipv6 address ipv6-address`
6. `ipv6 traffic-filter access-list-name {in | out}`
7. `end`
8. `show running-config`
9. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Security

#### Monitoring IPv6 ACLs

You can display information about all configured access lists, all IPv6 access lists, or a specific access list by using one or more of the privileged EXEC commands shown in the table below:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show access-lists</code></td>
<td>Displays all access lists configured on the switch.</td>
</tr>
<tr>
<td><code>show ipv6 access-list [access-list-name]</code></td>
<td>Displays all configured IPv6 access lists or the access list specified by name.</td>
</tr>
</tbody>
</table>

This is an example of the output from the `show access-lists` privileged EXEC command. The output shows all access lists that are configured on the switch.
This is an example of the output from the `show ipv6 access-list` privileged EXEC command. The output shows only IPv6 access lists configured on the switch.

```
Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30
IPv6 access list outbound
  deny udp any any sequence 10
  deny tcp any any eq telnet sequence 20
```

**Configuring PACL Mode and Applying IPv6 PACL on an Interface**

**Before you begin**

Before you configure the IPv6 PACL feature, you must configure an IPv6 access list. Once you have configured the IPv6 access list, you must configure the port-based access control list (PACL) mode on the specified IPv6 Layer 2 interface.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ipv6 access-list access-list-name
4. exit
5. interface type number
6. ipv6 traffic-filter access-list-name {in | out}
7. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 access-list access-list-name</td>
<td>Defines an IPv6 ACL and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# ipv6 access-list list1</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
Step 4 | exit
Example: Device(config-ipv6-acl)# exit
Exits IPv6 access list configuration mode and enters global configuration mode.

Step 5 | interface type number
Example: Specifies an interface type and number and enters interface configuration mode.

Step 6 | ipv6 traffic-filter access-list-name {in | out}
Example: Filters incoming and outgoing IPv6 traffic on an interface.

Step 7 | end
Example: Exits interface configuration mode and enters privileged EXEC mode.

### Configuring IPv6 ACL Extensions for Hop by Hop Filtering

#### SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 access-list access-list-name
4. permit protocol \{source-ipv6-prefix|prefix-length | any | host source-ipv6-address | auth\} [operator [port-number]] \{destination-ipv6-prefix|prefix-length | any | host destination-ipv6-address | auth\} [operator [port-number]] \{dest-option-type [header-number | header-type]] [dscp value] [flow-label value] [fragments] [hbh] [log] [log-input] [mobility] [mobility-type [mh-number | mh-type]] [reflect name [timeout value]] [routing] [routing-type routing-number] [sequence value] [time-range name] [undetermined-transport]
5. deny protocol \{source-ipv6-prefix|prefix-length | any | host source-ipv6-address | auth\} [operator [port-number]] \{destination-ipv6-prefix|prefix-length | any | host destination-ipv6-address | auth\} [operator [port-number]] \{dest-option-type [header-number | header-type]] [dscp value] [flow-label value] [fragments] [hbh] [log] [log-input] [mobility] [mobility-type [mh-number | mh-type]] [routing] [routing-type routing-number] [sequence value] [time-range name] [undetermined-transport]
6. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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. |
### Purpose

Command or Action | Purpose
--- | ---
**Step 3** | ipv6 access-list  *access-list-name*  
Example:  
Device(config)# ipv6 access-list hbh-acl  
| Defines an IPv6 ACL and enters IPv6 access list configuration mode.

**Step 4** | permit protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address | auth} [operator [port-number]]  
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address | auth} [operator [port-number]]  
[dest-option-type [header-number | header-type]] [dscp value] [flow-label value] [fragments] [hhb] [log]  
[log-input] [mobility] [mobility-type [mh-number | mh-type]] [reflect name [timeout value]] [routing]  
[routing-type routing-number] [sequence value] [time-range name]  
Example:  
Device(config-ipv6-acl)# permit icmp any any dest-option-type  
| Sets permit conditions for the IPv6 ACL.

**Step 5** | deny protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address | auth} [operator [port-number]]  
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address | auth} [operator [port-number]]  
[dest-option-type [header-number | header-type]] [dscp value] [flow-label value] [fragments] [hhb] [log]  
[log-input] [mobility] [mobility-type [mh-number | mh-type]] [reflect name [timeout value]] [routing]  
[routing-type routing-number] [sequence value] [time-range name] [undetermined-transport]  
Example:  
Device(config-ipv6-acl)# deny icmp any any dest-option-type  
| Sets deny conditions for the IPv6 ACL.

**Step 6** | end  
Example:  
Device (config-ipv6-acl)# end  
| Returns to privileged EXEC configuration mode.

## Configuration Examples for IPv6 ACLs

### Example: Configuring IPv6 ACLs

This example configures the IPv6 access list named CISCO. The first deny entry in the list denies all packets that have a destination TCP port number greater than 5000. The second deny entry denies packets that have a source UDP port number less than 5000. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets. The second permit entry in the list permits all other traffic.
The second permit entry is necessary because an implicit deny -all condition is at the end of each IPv6 access list.

Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch(config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any

Example: Configuring PACL Mode and Applying IPv6 PACL on an Interface

Device# configure terminal
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)# exit
Device(config-if)# ipv6 traffic-filter list1 in

Example: IPv6 ACL Extensions for Hop by Hop Filtering

Device(config)# ipv6 access-list hbh_acl
Device(config-ipv6-acl)# permit tcp any any hbh
Device(config-ipv6-acl)# permit tcp any any
Device(config-ipv6-acl)# permit udp any any
Device(config-ipv6-acl)# permit udp any any hbh
Device(config-ipv6-acl)# permit hbh any any
Device(config-ipv6-acl)# permit any any
Device(config-ipv6-acl)# hardware statistics
Device(config-ipv6-acl)# exit

! Assign an IP address and add the ACL on the interface.

Device(config)# interface FastEthernet3/1
Device(config-if)# ipv6 address 1001::1/64
Device(config-if)# ipv6 traffic-filter hbh_acl in
Device(config-if)# exit
Device(config)# exit
Device# clear counters
Clear "show interface" counters on all interfaces [confirm]
Device#

! Verify the configurations.

Device# show running-config interface FastEthernet3/1

Building configuration...

Current configuration : 114 bytes
!
interface FastEthernet3/1
no switchport
ipv6 address 1001::1/64
ipv6 traffic-filter hbh_acl
end
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

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

Feature Information for IPv6 Access Control Lists

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Table 82: Feature Information for IPv6 Access Control Lists

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 ACL Extensions for Hop-by-Hop Filtering</td>
<td>15.1(1)SG</td>
<td>Allows you to control IPv6 traffic that might contain hop-by-hop extension headers. This feature was supported on CAT3560C, CAT3560CX, CAT3560X, CAT3750X, CAT4500-X. The following commands were introduced or modified: <code>deny (IPv6)</code>, <code>permit (IPv6)</code>.</td>
</tr>
<tr>
<td>IPv6 PACL Support</td>
<td></td>
<td>The IPv6 PACL feature permits or denies the movement of traffic between port-based interface, Layer 3 subnets, wireless or wired clients, and VLANs, or within a VLAN. This feature was supported on CAT2960, CAT2960S, CAT3560X, CAT3650, CAT3560CX, CAT4500. The following command was introduced or modified: <code>ipv6 traffic-filter</code>.</td>
</tr>
<tr>
<td>IPv6 Services: Extended Access Control Lists</td>
<td>12.2(25)SG</td>
<td>Standard IPv6 ACL functionality was extended to support traffic filtering based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control.</td>
</tr>
<tr>
<td>IPv6 Services: Standard Access Control Lists</td>
<td>12.2(25)SG</td>
<td>Access lists determine what traffic is blocked and what traffic is forwarded at router interfaces and allow filtering based on source and destination addresses, inbound and outbound to a specific interface.</td>
</tr>
</tbody>
</table>
Feature Information for IPv6 Access Control Lists
Configuring DHCP

- Finding Feature Information, on page 799
- Information About DHCP, on page 799
- How to Configure DHCP Features, on page 806
- Configuring DHCP Server Port-Based Address Allocation, on page 815

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About DHCP

DHCP Server

The DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator. The switch can act as a DHCP server.

DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces.
DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Note

For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

An untrusted DHCP message is a message that is received through an untrusted interface. By default, the switch considers all interfaces untrusted. So, the switch must be configured to trust some interfaces to use DHCP Snooping. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer’s switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, an example of an interface you might configure as trusted is one connected to a port on a device in the same network. An example of an untrusted interface is one that is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.

If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.
When an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the `ip dhcp snooping information option allow-untrusted` global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as dynamic ARP inspection or IP source guard, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on untrusted input interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

Normally, it is not desirable to broadcast packets to wireless clients. So, DHCP snooping replaces destination broadcast MAC address (ffff.ffff.ffff) with unicast MAC address for DHCP packets that are going from server to wireless clients. The unicast MAC address is retrieved from CHADDR field in the DHCP payload. This processing is applied for server to client packets such as DHCP OFFER, DHCP ACK, and DHCP NACK messages. The `ip dhcp snooping wireless bootp-broadcast enable` can be used to revert this behavior. When the wireless BOOTP broadcast is enabled, the broadcast DHCP packets from server are forwarded to wireless clients without changing the destination MAC address.

**Related Topics**

Prerequisites for Configuring DHCP Snooping and Option 82, on page 810

### Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

---

**Note**

The DHCP option-82 feature is supported only when DHCP snooping is globally enabled on the VLANs to which subscriber devices using option-82 are assigned.

The following illustration shows a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

**Figure 55: DHCP Relay Agent in a Metropolitan Ethernet Network**
When you enable the DHCP snooping information option 82 on the switch, the following sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.

- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier, `vlan-mod-port`, from which the packet is received. You can configure the remote ID and circuit ID.

- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.

- The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

- The DHCP server receives the packet. If the server is option-82-capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.

- The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

In the default suboption configuration, when the described sequence of events occurs, the values in these fields do not change (see the illustration, *Suboption Packet Formats*):

- Circuit-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Circuit-ID type
  - Length of the circuit-ID type

- Remote-ID suboption fields
  - Suboption type
  - Length of the suboption type
  - Remote-ID type
  - Length of the remote-ID type

In the port field of the circuit ID suboption, the port numbers start at 3. For example, on a switch with 24 10/100/1000 ports and four small form-factor pluggable (SFP) module slots, port 3 is the Gigabit Ethernet 1/0/1 port, port 4 is the Gigabit Ethernet 1/0/2 port, and so forth. Port 27 is the SFP module slot Gigabit Ethernet1/0/25, and so forth.

The illustration, *Suboption Packet Formats*, shows the packet formats for the remote-ID suboption and the circuit-ID suboption when the default suboption configuration is used. The switch uses the packet formats when you globally enable DHCP snooping and enter the `ip dhcp snooping information option global` configuration command.
The illustration, *User-Configured Suboption Packet Formats*, shows the packet formats for user-configured remote-ID and circuit-ID suboptions. The switch uses these packet formats when DHCP snooping is globally enabled and when the `ip dhcp snooping information option format remote-id` global configuration command and the `ip dhcp snooping vlan information option format-type circuit-id string` interface configuration command are entered.

The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:

- **Circuit-ID suboption fields**
  - The circuit-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.

- **Remote-ID suboption fields**
  - The remote-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.
Cisco IOS DHCP Server Database

During the DHCP-based autoconfiguration process, the designated DHCP server uses the Cisco IOS DHCP server database. It has IP addresses, address bindings, and configuration parameters, such as the boot file.

An address binding is a mapping between an IP address and a MAC address of a host in the Cisco IOS DHCP server database. You can manually assign the client IP address, or the DHCP server can allocate an IP address from a DHCP address pool. For more information about manual and automatic address bindings, see the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.4.

For procedures to enable and configure the Cisco IOS DHCP server database, see the “DHCP Configuration Task List” section in the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.4.

DHCP Snooping Binding Database

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 64,000 bindings.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP inspection or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch updates the file when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is
updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file with bindings:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
<entry-n> <checksum-1-2-..-n>
END
```

Each entry in the file is tagged with a checksum value that the switch uses to verify the entries when it reads the file. The initial-checksum entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

When the switch starts and the calculated checksum value equals the stored checksum value, the switch reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The switch ignores an entry when one of these situations occurs:

- The switch reads the entry and the calculated checksum value does not equal the stored checksum value. The entry and the ones following it are ignored.
- An entry has an expired lease time (the switch might not remove a binding entry when the lease time expires).
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.
# How to Configure DHCP Features

## Default DHCP Snooping Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
</table>
| DHCP server                                  | Enabled in Cisco IOS software, requires configuration.  
8 |                                                                                   |
| DHCP relay agent                             | Enabled2                                                                         |
| DHCP packet forwarding address               | None configured                                                                 |
| Checking the relay agent information         | Enabled (invalid messages are dropped)                                           |
| DHCP relay agent forwarding policy           | Replace the existing relay agent information                                     |
| DHCP snooping enabled globally               | Disabled                                                                        |
| DHCP snooping information option             | Enabled                                                                         |
| DHCP snooping option to accept packets on untrusted input interfaces10 | Disabled                                                                        |
| DHCP snooping limit rate                     | None configured                                                                 |
| DHCP snooping trust                           | Untrusted                                                                       |
| DHCP snooping VLAN                            | Disabled                                                                        |
| DHCP snooping MAC address verification       | Enabled                                                                         |
| Cisco IOS DHCP server binding database       | Enabled in Cisco IOS software, requires configuration.  
Note: The switch gets network addresses and configuration parameters only from a device configured as a DHCP server. |
| DHCP snooping binding database agent         | Enabled in Cisco IOS software, requires configuration.  
This feature is operational only when a destination is configured. |

8  The switch responds to DHCP requests only if it is configured as a DHCP server.
9  The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
10 Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.
DHCP Snooping Configuration Guidelines

- If a switch port is connected to a DHCP server, configure a port as trusted by entering the `ip dhcp snooping trust interface` configuration command.

- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the `no ip dhcp snooping trust interface` configuration command.

- You can display DHCP snooping statistics by entering the `show ip dhcp snooping statistics` user EXEC command, and you can clear the snooping statistics counters by entering the `clear ip dhcp snooping statistics` privileged EXEC command.

Configuring the DHCP Server

The switch can act as a DHCP server.
For procedures to configure the switch as a DHCP server, see the “Configuring DHCP” section of the “IP addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.4.

Configuring the DHCP Relay Agent

Follow these steps to enable the DHCP relay agent on the switch:

### SUMMARY STEPS
1. `enable`
2. `configure terminal`
3. `service dhcp`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>service dhcp</code></td>
<td>Enables the DHCP server and relay agent on your switch. By default, this feature is enabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the switch with the `ip helper-address address` interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the `ip helper-address` command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface vlan vlan-id`
4. `ip address ip-address subnet-mask`
5. `ip helper-address address`
6. `end`
7. Use one of the following:
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates a switch virtual interface by entering a VLAN ID, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>interface vlan vlan-id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface vlan 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the interface with an IP address and an IP subnet.</td>
</tr>
<tr>
<td><code>ip address ip-address subnet-mask</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# ip address 192.108.1.27 255.255.255.0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specifies the DHCP packet forwarding address.</td>
</tr>
<tr>
<td><code>ip helper-address address</code></td>
<td>The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests. If you have multiple servers, you can configure one helper address for each server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# ip helper-address 172.16.1.2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 7</strong> Use one of the following: • <strong>interface range</strong> port-range • <strong>interface</strong> interface-id</td>
<td>Configures multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. or Configures a single physical port that is connected to the DHCP client, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet1/0/2</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> <strong>switchport mode access</strong></td>
<td>Defines the VLAN membership mode for the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> <strong>switchport access vlan</strong> vlan-id</td>
<td>Assigns the ports to the same VLAN as configured in Step 2.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport access vlan 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> <strong>end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> <strong>show running-config</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> <strong>copy running-config startup-config</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisites for Configuring DHCP Snooping and Option 82**

The prerequisites for DHCP Snooping and Option 82 are as follows:

- You must globally enable DHCP snooping on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- If you want the switch to respond to DHCP requests, it must be configured as a DHCP server.
Before configuring the DHCP snooping information option on your switch, be sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.

For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces. In a service-provider network, a trusted interface is connected to a port on a device in the same network.

You must configure the switch to use the Cisco IOS DHCP server binding database to use it for DHCP snooping.

To use the DHCP snooping option of accepting packets on untrusted inputs, the switch must be an aggregation switch that receives packets with option-82 information from an edge switch.

The following prerequisites apply to DHCP snooping binding database configuration:

- You must configure a destination on the DHCP snooping binding database to use the switch for DHCP snooping.
- Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store the binding file on a TFTP server.
- For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the switch can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.
- To ensure that the lease time in the database is accurate, we recommend that you enable and configure Network Time Protocol (NTP).
- If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.

If you want the switch to relay DHCP packets, the IP address of the DHCP server must be configured on the switch virtual interface (SVI) of the DHCP client.

If a switch port is connected to a DHCP server, configure a port as trusted by entering the `ip dhcp snooping trust interface` configuration command.

If a switch port is connected to a DHCP client, configure a port as untrusted by entering the `no ip dhcp snooping trust` interface configuration command.

**Related Topics**

[DHCP Snooping](#), on page 800

---

**Enabling DHCP Snooping and Option 82**

Follow these steps to enable DHCP snooping on the switch:
### SUMMARY STEPS

1. enable
2. configure terminal
3. ip dhcp snooping
4. ip dhcp snooping vlan `vlan-range`
5. ip dhcp snooping information option
6. ip dhcp snooping information option format remote-id [string `ASCII-string` | hostname]
7. ip dhcp snooping information option allow-untrusted
8. interface `interface-id`
9. ip dhcp snooping vlan `vlan information option format-type circuit-id [override] string `ASCII-string`
10. ip dhcp snooping trust
11. ip dhcp snooping limit rate `rate`
12. exit
13. ip dhcp snooping verify mac-address
14. end
15. show running-config
16. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip dhcp snooping</td>
<td>Enables DHCP snooping globally.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip dhcp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip dhcp snooping vlan <code>vlan-range</code></td>
<td>Enables DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip dhcp snooping vlan 10</td>
<td>• You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens,</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip dhcp snooping information option</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 6</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Configures the remote-ID suboption.</td>
</tr>
<tr>
<td></td>
<td>You can configure the remote ID as:</td>
</tr>
<tr>
<td></td>
<td>• String of up to 63 ASCII characters (no spaces)</td>
</tr>
<tr>
<td></td>
<td>• Configured hostname for the switch</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The default remote ID is the switch MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) If the switch is an aggregation switch connected to an edge switch, this command enables the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch.</td>
</tr>
<tr>
<td></td>
<td>The default setting is disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Step 8</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 9</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Configures the circuit-ID suboption for the specified interface.</td>
</tr>
<tr>
<td></td>
<td>Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094. The default circuit ID is the port identifier, in the format <strong>vlan-mod-port</strong>.</td>
</tr>
<tr>
<td></td>
<td>You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces).</td>
</tr>
<tr>
<td></td>
<td>(Optional) Use the <strong>override</strong> keyword when you do not want the circuit-ID suboption inserted in TLV format to define subscriber information.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 10</td>
<td>ip dhcp snooping trust</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# ip dhcp snooping trust</td>
</tr>
<tr>
<td>Step 11</td>
<td>ip dhcp snooping limit rate <code>rate</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# ip dhcp snooping limit rate 100</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>exit</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# exit</td>
</tr>
<tr>
<td>Step 13</td>
<td>ip dhcp snooping verify mac-address</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip dhcp snooping verify mac-address</td>
</tr>
<tr>
<td>Step 14</td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>Step 15</td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
</tr>
<tr>
<td>Step 16</td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Enabling the Cisco IOS DHCP Server Database

For procedures to enable and configure the Cisco IOS DHCP server database, see the “DHCP Configuration Task List” section in the “Configuring DHCP” chapter of the Cisco IOS IP Configuration Guide, Release 12.4

Monitoring DHCP Snooping Information

<table>
<thead>
<tr>
<th>Table 84: Commands for Displaying DHCP Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip dhcp snooping</strong></td>
</tr>
<tr>
<td><strong>show ip dhcp snooping binding</strong></td>
</tr>
<tr>
<td><strong>show ip dhcp snooping database</strong></td>
</tr>
<tr>
<td><strong>show ip dhcp snooping statistics</strong></td>
</tr>
<tr>
<td><strong>show ip source binding</strong></td>
</tr>
</tbody>
</table>

Note: If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Configuring DHCP Server Port-Based Address Allocation

Information About Configuring DHCP Server Port-Based Address Allocation

DHCP server port-based address allocation is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port regardless of the attached device client identifier or client hardware address.

When Ethernet switches are deployed in the network, they offer connectivity to the directly connected devices. In some environments, such as on a factory floor, if a device fails, the replacement device must be working immediately in the existing network. With the current DHCP implementation, there is no guarantee that DHCP would offer the same IP address to the replacement device. Control, monitoring, and other software expect a stable IP address associated with each device. If a device is replaced, the address assignment should remain stable even though the DHCP client has changed.

When configured, the DHCP server port-based address allocation feature ensures that the same IP address is always offered to the same connected port even as the client identifier or client hardware address changes in the DHCP messages received on that port. The DHCP protocol recognizes DHCP clients by the client identifier
option in the DHCP packet. Clients that do not include the client identifier option are identified by the client hardware address. When you configure this feature, the port name of the interface overrides the client identifier or hardware address and the actual point of connection, the switch port, becomes the client identifier.

In all cases, by connecting the Ethernet cable to the same port, the same IP address is allocated through DHCP to the attached device.

The DHCP server port-based address allocation feature is only supported on a Cisco IOS DHCP server and not a third-party server.

**Default Port-Based Address Allocation Configuration**

By default, DHCP server port-based address allocation is disabled.

**Port-Based Address Allocation Configuration Guidelines**

- By default, DHCP server port-based address allocation is disabled.
- To restrict assignments from the DHCP pool to preconfigured reservations (unreserved addresses are not offered to the client and other clients are not served by the pool), you can enter the reserved-only DHCP pool configuration command.

**Enabling the DHCP Snooping Binding Database Agent**

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the switch:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip dhcp snooping database {flash[number]://filename | ftp://user:password@host//filename | http://[(username:password@)[\] host-name | host-ip]//directory/image-name.tar | rcp://user@host//filename]} | tftp://host//filename
4. ip dhcp snooping database timeout seconds
5. ip dhcp snooping database write-delay seconds
6. end
7. ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds
8. show ip dhcp snooping database [detail]
9. show running-config
10. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <strong>enable</strong></td>
<td>- Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip dhcp snooping database {flash[number]:/filename</td>
<td>ftp://user:password@host/filename</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2</td>
<td>Specifies the URL for the database agent or the binding file by using one of these forms:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip dhcp snooping database timeout seconds</td>
<td>Specifies (in seconds) how long to wait for the database transfer process to finish before stopping the process. The default is 300 seconds. The range is 0 to 86400. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping database timeout 300</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip dhcp snooping database write-delay seconds</td>
<td>Specifies the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping database write-delay 15</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</td>
<td>(Optional) Adds binding entries to the DHCP snooping binding database. The vlan-id range is from 1 to 4904. The seconds range is from 1 to 4294967295. Enter this command for each entry that you add. Use this command when you are testing or debugging the switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000</td>
<td></td>
</tr>
</tbody>
</table>
Enabling DHCP Server Port-Based Address Allocation

Follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip dhcp use subscriber-id client-id
4. ip dhcp subscriber-id interface-name
5. interface interface-id
6. ip dhcp server use subscriber-id client-id
7. end
8. show running-config
9. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| Example:          |         |
| Switch> enable    |         |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:          |         |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>ip dhcp use subscriber-id client-id</code></td>
<td>Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.</td>
</tr>
</tbody>
</table>
|      | Example:  
  Switch(config)# `ip dhcp use subscriber-id client-id` | |
| 4    | `ip dhcp subscriber-id interface-name` | Automatically generates a subscriber identifier based on the short name of the interface. A subscriber identifier configured on a specific interface takes precedence over this command. |
|      | Example:  
  Switch(config)# `ip dhcp subscriber-id interface-name` | |
| 5    | `interface interface-id` | Specifies the interface to be configured, and enter interface configuration mode. |
|      | Example:  
  Switch(config)# `interface gigabitethernet 0/1` | |
| 6    | `ip dhcp server use subscriber-id client-id` | Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface. |
|      | Example:  
  Switch(config-if)# `ip dhcp server use subscriber-id client-id` | |
| 7    | `end` | Returns to privileged EXEC mode. |
|      | Example:  
  Switch(config)# `end` | |
| 8    | `show running-config` | Verifies your entries. |
|      | Example:  
  Switch# `show running-config` | |
| 9    | `copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
|      | Example:  
  Switch# `copy running-config startup-config` | |

### What to do next

After enabling DHCP port-based address allocation on the switch, use the `ip dhcp pool` global configuration command to preassign IP addresses and to associate them to clients.
Monitoring DHCP Server Port-Based Address Allocation

Table 85: Commands for Displaying DHCP Port-Based Address Allocation Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface interface id</td>
<td>Displays the status and configuration of a specific interface.</td>
</tr>
<tr>
<td>show ip dhcp pool</td>
<td>Displays the DHCP address pools.</td>
</tr>
<tr>
<td>show ip dhcp binding</td>
<td>Displays address bindings on the Cisco IOS DHCP server.</td>
</tr>
</tbody>
</table>

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
</tr>
</tbody>
</table>

Link: http://www.cisco.com/support
## Feature Information for DHCP Snooping and Option 82

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

Introduced support for the following commands:

- `show ip dhcp snooping statistics` user EXEC command for displaying DHCP snooping statistics.
- `clear ip dhcp snooping statistics` privileged EXEC command for clearing the snooping statistics counters.
Feature Information for DHCP Snooping and Option 82
CHAPTER 46

Configuring IEEE 802.1x Port-Based Authentication

This chapter describes how to configure IEEE 802.1x port-based authentication. IEEE 802.1x authentication prevents unauthorized devices (clients) from gaining access to the network. Unless otherwise noted, the term switch refers to a standalone switch.

- Finding Feature Information, on page 823
- How to Configure 802.1x Port-Based Authentication, on page 823
- Monitoring 802.1x Statistics and Status, on page 859
- Additional References, on page 860
- Feature Information for 802.1x Port-Based Authentication, on page 861

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

How to Configure 802.1x Port-Based Authentication

Default 802.1x Authentication Configuration

Table 86: Default 802.1x Authentication Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 802.1x enable state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Per-port 802.1x enable state</td>
<td>Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.</td>
</tr>
<tr>
<td>AAA</td>
<td>Disabled.</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>• None specified.</td>
</tr>
<tr>
<td>• IP address</td>
<td>• 1645.</td>
</tr>
<tr>
<td>• UDP authentication port</td>
<td>• 1646.</td>
</tr>
<tr>
<td>• Default accounting port</td>
<td>• None specified.</td>
</tr>
<tr>
<td>• Key</td>
<td></td>
</tr>
<tr>
<td>Host mode</td>
<td>Single-host mode.</td>
</tr>
<tr>
<td>Control direction</td>
<td>Bidirectional control.</td>
</tr>
<tr>
<td>Periodic re-authentication</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Number of seconds between re-authentication attempts</td>
<td>3600 seconds.</td>
</tr>
<tr>
<td>Re-authentication number</td>
<td>2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).</td>
</tr>
<tr>
<td>Retransmission time</td>
<td>30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before resending the request).</td>
</tr>
<tr>
<td>Maximum retransmission number</td>
<td>2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).</td>
</tr>
<tr>
<td>Client timeout period</td>
<td>30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before resending the request to the client.)</td>
</tr>
<tr>
<td>Authentication server timeout period</td>
<td>30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before resending the response to the server.) You can change this timeout period by using the dot1x timeout server-timeout interface configuration command.</td>
</tr>
</tbody>
</table>
### 802.1x Authentication Configuration Guidelines

#### 802.1x Authentication

These are the 802.1x authentication configuration guidelines:

- When 802.1x authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.

- If the VLAN to which an 802.1x-enabled port is assigned changes, this change is transparent and does not affect the switch. For example, this change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after re-authentication.

If the VLAN to which an 802.1x port is assigned to shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.

- The 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports, but it is not supported on these port types:
  - Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x authentication on a dynamic port, an error message appears, and 802.1x authentication is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
  - EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x authentication on an EtherChannel port, an error message appears, and 802.1x authentication is not enabled.
  - Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1x authentication on a port that is a SPAN or RSPAN destination port. However, 802.1x authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable 802.1x authentication on a SPAN or RSPAN source port.

- Before globally enabling 802.1x authentication on a switch by entering the `dot1x system-auth-control` global configuration command, remove the EtherChannel configuration from the interfaces on which 802.1x authentication and EtherChannel are configured.

### Table: Default Setting of 802.1x Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity timeout</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Inaccessible authentication bypass</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Restricted VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Authenticator (switch) mode</td>
<td>None specified.</td>
</tr>
<tr>
<td>MAC authentication bypass</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Voice-aware security</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>
Cisco IOS Release 12.2(55)SE and later supports filtering of system messages related to 802.1x authentication.

**VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass**

These are the configuration guidelines for VLAN assignment, guest VLAN, restricted VLAN, and inaccessible authentication bypass:

- When 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- The 802.1x authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.
- You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- After you configure a guest VLAN for an 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the 802.1x authentication process (authentication timer inactivity and authentication timer reauthentication) interface configuration commands). The amount to decrease the settings depends on the connected 802.1x client type.
- When configuring the inaccessible authentication bypass feature, follow these guidelines:
  - The feature is supported on 802.1x port in single-host mode and multihosts mode.
  - If the client is running Windows XP and the port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.
  - If the Windows XP client is configured for DHCP and has an IP address from the DHCP server, receiving an EAP-Success message on a critical port might not re-initiate the DHCP configuration process.
  - You can configure the inaccessible authentication bypass feature and the restricted VLAN on an 802.1x port. If the switch tries to re-authenticate a critical port in a restricted VLAN and all the RADIUS servers are unavailable, switch changes the port state to the critical authentication state and remains in the restricted VLAN.
  - If the CTS links are in Critical Authentication mode and the master reloads, the policy where SGT was configured on a device will not be available on the new master. This is because the internal bindings will not be synced to the standby switch in a 3750-X switch stack.
  - You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
  - When wireless guest clients obtains IP from foreign client VLAN instead of anchor client VLAN, you should use the `ip dhcp required` command under the WLAN configuration to force clients to issue a new DHCP request. This prevents the clients from getting an incorrect IP at anchor.
MAC Authentication Bypass

These are the MAC authentication bypass configuration guidelines:

- Unless otherwise stated, the MAC authentication bypass guidelines are the same as the 802.1x authentication guidelines.

- If you disable MAC authentication bypass from a port after the port has been authorized with its MAC address, the port state is not affected.

- If the port is in the unauthorized state and the client MAC address is not the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to re-authorize the port.

- If the port is in the authorized state, the port remains in this state until re-authorization occurs.

- You can configure a timeout period for hosts that are connected by MAC authentication bypass but are inactive. The range is 1 to 65535 seconds.

Maximum Number of Allowed Devices Per Port

This is the maximum number of devices allowed on an 802.1x-enabled port:

- In single-host mode, only one device is allowed on the access VLAN. If the port is also configured with a voice VLAN, an unlimited number of Cisco IP phones can send and receive traffic through the voice VLAN.

- In multidomain authentication (MDA) mode, one device is allowed for the access VLAN, and one IP phone is allowed for the voice VLAN.

- In multihost mode, only one 802.1x supplicant is allowed on the port, but an unlimited number of non-802.1x hosts are allowed on the access VLAN. An unlimited number of devices are allowed on the voice VLAN.

Configuring 802.1x Violation Modes

You can configure an 802.1x port so that it shuts down, generates a syslog error, or discards packets from a new device when:

- a device connects to an 802.1x-enabled port
- the maximum number of allowed about devices have been authenticated on the port

Beginning in privileged EXEC mode, follow these steps to configure the security violation actions on the switch:

SUMMARY STEPS

1. configure terminal
2. aaa new-model
3. aaa authentication dot1x {default} method1
4. interface interface-id
5. switchport mode access
6. authentication violation {shutdown | restrict | protect | replace}
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>aaa authentication dot1x {default} method1</code></td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# aaa authentication dot1x default group radius</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To create a default list that is used when a named list is <em>not</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>specified in the <code>authentication</code> command, use the <code>default</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>keyword followed by the method that is to be used in default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>situations. The default method list is automatically applied to all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For <code>method1</code>, enter the <code>group radius</code> keywords to use the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface interface-id</code></td>
<td>Specifies the port connected to the client that is to be</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet 0/4</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet 1/0/4</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>switchport mode access</code></td>
<td>Sets the port to access mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>`authentication violation {shutdown</td>
<td>restrict</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>meanings:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>shutdown</code>– Error disable the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>restrict</code>– Generate a syslog error.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>protect</code>– Drop packets from any new device that sends</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traffic to the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>replace</code>– Removes the current session and authenticates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with the new host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.1x Authentication

To allow per-user ACLs or VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

This is the 802.1x AAA process:

**Before you begin**

To configure 802.1x port-based authentication, you must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

**SUMMARY STEPS**

1. A user connects to a port on the switch.
2. Authentication is performed.
3. VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.
4. The switch sends a start message to an accounting server.
5. Re-authentication is performed, as necessary.
6. The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.
7. The user disconnects from the port.
8. The switch sends a stop message to the accounting server.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>A user connects to a port on the switch.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Authentication is performed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>The switch sends a start message to an accounting server.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Re-authentication is performed, as necessary.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>The user disconnects from the port.</td>
</tr>
</tbody>
</table>
### Configuring 802.1x Port-Based Authentication

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication:

**SUMMARY STEPS**

1. `configure terminal`
2. `aaa new-model`
3. `aaa authentication dot1x {default} method1`
4. `dot1x system-auth-control`
5. `aaa authorization network {default} group radius`
6. `radius-server host ip-address`
7. `radius-server key string`
8. `interface interface-id`
9. `switchport mode access`
10. `authentication port-control auto`
11. `dot1x pae authenticator`
12. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>aaa new-model</code></td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>aaa authentication dot1x {default} method1</code></td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# aaa authentication dot1x default group radius</code></td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To create a default list that is used when a named list is not specified in the <code>authentication</code> command, use the <code>default</code> keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For <code>method1</code>, enter the <code>group radius</code> keywords to use the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables 802.1x authentication globally on the switch.</td>
<td></td>
</tr>
<tr>
<td><code>dot1x system-auth-control</code></td>
<td>Enables 802.1x authentication globally on the switch.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enables 802.1x authentication globally on the switch.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# dot1x system-auth-control</code></td>
<td>Enables 802.1x authentication globally on the switch.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</td>
<td></td>
</tr>
<tr>
<td><code>aaa authorization network (default) group radius</code></td>
<td>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization network default group radius</code></td>
<td>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><code>radius-server host ip-address</code></td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# radius-server host 124.2.2.12</code></td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><code>radius-server key string</code></td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# radius-server key abc1234</code></td>
<td>(Optional) Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 0/2</code></td>
<td>Specifies the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>(Optional) Sets the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.</td>
<td></td>
</tr>
<tr>
<td><code>switchport mode access</code></td>
<td>(Optional) Sets the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Sets the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td>(Optional) Sets the port to access mode only if you configured the RADIUS server in Step 6 and Step 7.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Enables 802.1x authentication on the port.</td>
<td></td>
</tr>
<tr>
<td><code>authentication port-control auto</code></td>
<td>Enables 802.1x authentication on the port.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Enables 802.1x authentication on the port.</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# authentication port-control auto</code></td>
<td>Enables 802.1x authentication on the port.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the Switch-to-RADIUS-Server Communication

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the `radius-server host` global configuration command. If you want to configure these options on a per-server basis, use the `radius-server timeout`, the `radius-server retransmit`, and the `radius-server key` global configuration commands.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, see the RADIUS server documentation.

Follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

**Before you begin**

You must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `radius-server host {hostname | ip-address} auth-port port-number key string`
4. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

```
Switch# configure terminal
```

**Step 3**

```
radius-server host {hostname | ip-address} auth-port port-number key string
```

**Example:**

```
Switch(config)# radius-server host 125.5.5.43 auth-port 1645 key rad123
```

- **Purpose:** Configures the RADIUS server parameters.
  - For `hostname | ip-address`, specify the server name or IP address of the remote RADIUS server.
  - For `auth-port port-number`, specify the UDP destination port for authentication requests. The default is 1645. The range is 0 to 65536.
  - For `key string`, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.

  **Note:** Always configure the key as the last item in the `radius-server host` command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.

If you want to use multiple RADIUS servers, re-enter this command.

**Step 4**

```
end
```

**Example:**

```
Switch(config)# end
```

- **Purpose:** Returns to privileged EXEC mode.

### Related Topics

- **Switch-to-RADIUS-Server Communication**

---

### Configuring the Host Mode

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an IEEE 802.1x-authorized port that has the `authentication port-control` interface configuration command set to `auto`. Use the `multi-domain` keyword to configure and enable multidomain authentication (MDA), which allows both a host and a voice device, such as an IP phone (Cisco or non-Cisco), on the same switch port. This procedure is optional.

### SUMMARY STEPS

1. `configure terminal`
2. `interface interface-id`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the port to which multiple hosts are indirectly attached, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td>Example: <code>Switch(config)# interface gigabitethernet 0/1 interface gigabitethernet2/0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Allows multiple hosts (clients) on an 802.1x-authorized port. The keywords have these meanings:</td>
</tr>
<tr>
<td>`authentication host-mode [multi-auth</td>
<td>multi-domain</td>
</tr>
<tr>
<td>Example: <code>Switch(config-if)# authentication host-mode multi-host</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Example: <code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note**
- The `multi-auth` keyword is only available with the `authentication host-mode` command.
- The `multi-host` keyword is only available with the `authentication host-mode` command.
- You must configure the voice VLAN for the IP phone when the host mode is set to `multi-domain`.

Make sure that the `authentication port-control` interface configuration command is set to `auto` for the specified interface.
Configuring Periodic Re-Authentication

You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between attempts is 3600.

Beginning in privileged EXEC mode, follow these steps to enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts. This procedure is optional.

SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. authentication periodic
4. authentication timer {inactivity | reauthenticate | restart | unauthorized} value
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1 interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3 authentication periodic</td>
<td>Enables periodic re-authentication of the client, which is disabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication periodic</td>
<td></td>
</tr>
<tr>
<td>Step 4 authentication timer {}</td>
<td>Sets the number of seconds between re-authentication attempts.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication timer reauthenticate 180</td>
<td></td>
</tr>
</tbody>
</table>

The authentication timer keywords have these meanings:

- **inactivity**—Interval in seconds after which if there is no activity from the client then it is unauthorized
- **reauthenticate**—Time in seconds after which an automatic re-authentication attempt is initiated
Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. The **authentication timer restart** interface configuration command controls the idle period. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.

Beginning in privileged EXEC mode, follow these steps to change the quiet period. This procedure is optional.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `authentication timer restart seconds`
4. `end`
5. `show authentication sessions interface interface-id`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  - `configure terminal`
  **Example:**
  Switch# configure terminal |
  Enters global configuration mode. |
| **Step 2**
  - `interface interface-id`
  **Example:**
  Switch(config)# interface gigabitethernet 0/1
  Specifications the port to be configured, and enter interface configuration mode. |
Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then resends the frame.

Note

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to change the amount of time that the switch waits for client notification. This procedure is optional.

SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. authentication timer reauthenticate seconds
4. end
5. show authentication sessions interface interface-id
6. copy running-config startup-config
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> authentication timer reauthenticate seconds</td>
<td>Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 5.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# authentication timer reauthenticate 60</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show authentication sessions interface interface-id</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show authentication sessions interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.
You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the switch-to-client frame-retransmission number. This procedure is optional.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `dot1x max-reauth-req count`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>dot1x max-reauth-req count</code></td>
<td>Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# dot1x max-reauth-req 5</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Setting the Re-Authentication Number**

You can also change the number of times that the switch restarts the authentication process before the port changes to the unauthorized state.
You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the re-authentication number. This procedure is optional.

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. switchport mode access
4. dot1x max-req count
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# interface gigabitethernet 0/1interface gigabitethernet2/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport mode access</td>
<td>Sets the port to access mode only if you previously configured the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dot1x max-req count</td>
<td>Sets the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 0 to 10; the default is 2.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# dot1x max-req 4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring 802.1x Accounting

Enabling AAA system accounting with 802.1x accounting allows system reload events to be sent to the accounting RADIUS server for logging. The server can then infer that all active 802.1x sessions are closed.

Because RADIUS uses the unreliable UDP transport protocol, accounting messages might be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, this system message appears:

Accounting message %s for session %s failed to receive Accounting Response.

When the stop message is not sent successfully, this message appears:

00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and timestamps. To turn on these functions, enable logging of “Update/Watchdog packets from this AAA client” in your RADIUS server Network Configuration tab. Next, enable “CVS RADIUS Accounting” in your RADIUS server System Configuration tab.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x accounting after AAA is enabled on your switch. This procedure is optional.

SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. aaa accounting dot1x default start-stop group radius
4. aaa accounting system default start-stop group radius
5. end
6. show running-config
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet</td>
<td></td>
</tr>
</tbody>
</table>
Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/3interface gigabitethernet1/0/3</td>
<td>Enables 802.1x accounting using the list of all RADIUS servers.</td>
</tr>
<tr>
<td>Step 3 aaa accounting dot1x default start-stop group radius</td>
<td>Enables 802.1x accounting using the list of all RADIUS servers.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# aaa accounting dot1x default start-stop group radius</td>
<td></td>
</tr>
<tr>
<td>Step 4 aaa accounting system default start-stop group radius</td>
<td>(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# aaa accounting system default start-stop group radius</td>
<td></td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEc mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Guest VLAN

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAP request/identity frame. Clients that are 802.1x-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host or multiple-hosts mode.

Beginning in privileged EXEC mode, follow these steps to configure a guest VLAN. This procedure is optional.

### SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. authentication event no-response action authorize vlan vlan-id
DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet 0/2</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><code>authentication event no-response action authorize vlan vlan-id</code></td>
<td>Specifies an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# authentication event no-response action authorize vlan 2</code></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring a Restricted VLAN**

When you configure a restricted VLAN on a switch stack, clients that are IEEE 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode.

Beginning in privileged EXEC mode, follow these steps to configure a restricted VLAN. This procedure is optional.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `authentication port-control auto`
4. `authentication event fail action authorize vlan vlan-id`
5. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface gigabitethernet 0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> authentication port-control auto</td>
<td>Enables 802.1x authentication on the port.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> authentication event fail action authorize vlan vlan-id</td>
<td>Specifies an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# authentication event fail action authorize vlan 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Number of Authentication Attempts on a Restricted VLAN

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the `authentication event retry retry count` interface configuration command. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.

Beginning in privileged EXEC mode, follow these steps to configure the maximum number of allowed authentication attempts. This procedure is optional.

### SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. authentication port-control auto
4. authentication event fail action authorize vlan vlan-id
5. authentication event retry retry count
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 0/3</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>authentication port-control auto</td>
<td>Enables 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>authentication event fail action authorize vlan vlan-id</td>
<td>Specifies an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication event fail action authorize vlan 8</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>authentication event retry retry count</td>
<td>Specifies a number of authentication attempts to allow before a port moves to the restricted VLAN. The range is 1 to 3, and the default is 3.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication event retry 2</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

## Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN

Beginning in privileged EXEC mode, follow these steps to configure critical voice VLAN on a port and enable the inaccessible authentication bypass feature.
SUMMARY STEPS

1. configure terminal
2. aaa new-model
3. radius-server dead-criteria {time seconds } [tries number]
4. radius-serverdeadtimeminutes
5. radius-server host ip-address address [acct-port udp-port] [auth-port udp-port] [testusername name [idle-time time] [ignore-acct-port] [ignore auth-port]] [key string]
6. dot1x critical {eapol | recovery delay milliseconds}
7. interface interface-id
8. authentication event server dead action {authorize | reinitialize} vlan vlan-id
9. switchport voice vlan vlan-id
10. authentication event server dead action authorize voice
11. show authentication interface interface-id
12. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> radius-server dead-criteria {time seconds } [tries number]</td>
<td>Sets the conditions that determine when a RADIUS server is considered un-available or down (dead).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# radius-server dead-criteria time 20 tries 10</td>
<td>- <em>time</em> — 1 to 120 seconds. The switch dynamically determines a default <em>seconds</em> value between 10 and 60.</td>
</tr>
<tr>
<td></td>
<td>- <em>number</em> — 1 to 100 tries. The switch dynamically determines a default <em>tries</em> <em>number</em> between 10 and 100.</td>
</tr>
<tr>
<td><strong>Step 4</strong> radius-serverdeadtimeminutes</td>
<td>(Optional) Sets the number of minutes during which a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# radius-server deadtime 60</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> radius-server host ip-address address [acct-port udp-port] [auth-port udp-port] [testusername name] [idle-time time] [ignore-acct-port] [ignore auth-port] [key string]</td>
<td>(Optional) Configure the RADIUS server parameters by using these keywords:</td>
</tr>
</tbody>
</table>
### Command or Action

| **name**[idle-time time] [ignore-acct-port][ignore auth-port]] [key string] |

#### Purpose
- **acct-port udp-port**—Specify the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646.
- **auth-port udp-port**—Specify the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645.

#### Example:

```
Switch(config)# radius-server host 1.1.1.2
acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234
```

#### Note
- You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values.

- **test username name**—Enable automated testing of the RADIUS server status, and specify the username to be used.

- **idle-time time**—Set the interval of time in minutes after which the switch sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour).

- **ignore-acct-port**—Disable testing on the RADIUS-server accounting port.

- **ignore-auth-port**—Disable testing on the RADIUS-server authentication port.

- For **key string**, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.

  #### Note
  - Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.

You can also configure the authentication and encryption key by using the **radius-server key {0string | 7string | string}** global configuration command.

### Step 6

| dot1x critical {eapol | recovery delay milliseconds} |

#### Example:

```
Step 6
```

(Optional) Configure the parameters for inaccessible authentication bypass:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Switch(config)# dot1x critical eapol`  
`Switch(config)# dot1x critical recovery delay 2000` | - *eapol*—Specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.  
- *recovery delay*\(^{milliseconds}\)—Set the recovery delay period during which the switch waits to re-initialize a critical port when a RADIUS server that was unavailable becomes available. The range is from 1 to 10000 milliseconds. The default is 1000 milliseconds (a port can be re-initialized every second). |

**Step 7**  
*interface interface-id*  
**Example:**  
`Switch(config)# interface gigabitethernet 0/1`  
*Specify the port to be configured, and enter interface configuration mode.*

**Step 8**  
*authentication event server dead action {authorize | reinitialize} vlan vlan-id*  
**Example:**  
`Switch(config-if)# authentication event server dead action reinitialize vlan 20`  
*Use these keywords to move hosts on the port if the RADIUS server is unreachable:  
- *authorize*—Move any new hosts trying to authenticate to the user-specified critical VLAN.  
- *reinitialize*—Move all authorized hosts on the port to the user-specified critical VLAN.*

**Step 9**  
*switchport voice vlan vlan-id*  
**Example:**  
`Switch(config-if)# switchport voice vlan`  
*Specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6.*

**Step 10**  
*authentication event server dead action authorize voice*  
**Example:**  
`Switch(config-if)# authentication event server dead action authorize voice`  
*Configures critical voice VLAN to move data traffic on the port to the voice VLAN if the RADIUS server is unreachable.*

**Step 11**  
*show authentication interface interface-id*  
**Example:**  
`Switch(config-if)# do show authentication interface gigabit 1/0/1`  
*(Optional) Verify your entries.*

**Step 12**  
*copy running-config startup-config*  
**Example:**  
*(Optional) Verify your entries.*
Example

To return to the RADIUS server default settings, use the no radius-server dead-criteria, the no radius-server deadtime, and the no radius-server host global configuration commands. To disable inaccessible authentication bypass, use the no authentication event server dead action interface configuration command. To disable critical voice VLAN, use the no authentication event server dead action authorize voice interface configuration command.

Example of Configuring Inaccessible Authentication Bypass

This example shows how to configure the inaccessible authentication bypass feature:

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# dot1x critical recovery delay 2000
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# dot1x critical vlan 20
Switch(config-if)# end
```

Configuring 802.1x Authentication with WoL

Beginning in privileged EXEC mode, follow these steps to enable 802.1x authentication with WoL. This procedure is optional.

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. authentication control-direction {both | in}
4. end
5. show authentication sessions interface interface-id
6. copy running-config startup-config
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Example: <code>Switch# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Example: <code>Switch(config)# interface gigabitethernet2/0/3</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables 802.1x authentication with WoL on the port, and use these keywords to configure the port as bidirectional or unidirectional.</td>
</tr>
<tr>
<td>authentication control-direction {both</td>
<td>in}</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td>Example: <code>Switch(config-if)# end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>show authentication sessions interface interface-id</td>
<td>Example: <code>Switch# show authentication sessions interface gigabitethernet2/0/3</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>Example: <code>Switch# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

### Configuring MAC Authentication Bypass

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication bypass. This procedure is optional.

---

**Security**

**Configuring MAC Authentication Bypass**

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication bypass. This procedure is optional.
### SUMMARY STEPS

1. `configure terminal`
2. `interface interface-id`
3. `authentication port-control auto`
4. `mab [eap]`
5. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `configure terminal`  
          Example:  
          Switch# configure terminal | Enters global configuration mode. |
| Step 2 | `interface interface-id`  
          Example:  
          Switch(config)# interface gigabitethernet 0/1 | Specifies the port to be configured, and enter interface configuration mode. |
| Step 3 | `authentication port-control auto`  
          Example:  
          Switch(config-if)# authentication port-control auto | Enables 802.1x authentication on the port. |
| Step 4 | `mab [eap]`  
          Example:  
          Switch(config-if)# mab | Enables MAC authentication bypass.  
          (Optional) Use the `eap` keyword to configure the switch to use EAP for authorization. |
| Step 5 | `end`  
          Example:  
          Switch(config-if)# end | Returns to privileged EXEC mode. |

### Formatting a MAC Authentication Bypass Username and Password

Use the optional `mab request format` command to format the MAB username and password in a style accepted by the authentication server. The username and password are usually the MAC address of the client. Some authentication server configurations require the password to be different from the username.

Beginning in privileged EXEC mode, follow these steps to format MAC authentication bypass username and passwords.
### SUMMARY STEPS

1. configure terminal
2. mab request format attribute1 groupsize {1 | 2 | 4 | 12} [separator { - | : | .} {lowercase | uppercase}]
3. mab request format attribute2 {0 | 7} text
4. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>Purpose</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mab request format attribute1 groupsize {1</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# mab request format attribute1 groupsize 12</td>
</tr>
<tr>
<td>Purpose</td>
<td>Specifies the format of the MAC address in the User-Name attribute of MAB-generated Access-Request packets. 1—Sets the username format of the 12 hex digits of the MAC address. group size—The number of hex nibbles to concatenate before insertion of a separator. A valid group size must be either 1, 2, 4, or 12. separator—The character that separates the hex nibbles according to group size. A valid separator must be either a hyphen, colon, or period. No separator is used for a group size of 12. {lowercase</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>mab request format attribute2 {0</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# mab request format attribute 2 7 A02f44E18B12</td>
</tr>
<tr>
<td>Purpose</td>
<td>2—Specifies a custom (nondefault) value for the User-Password attribute in MAB-generated Access-Request packets. 0— Specifies a cleartext password to follow. 7— Specifies an encrypted password to follow. text— Specifies the password to be used in the User-Password attribute.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

When you send configuration information in e-mail, remove type 7 password information. The `show tech-support` command removes this information from its output by default.
Configuring Limiting Login for Users

SUMMARY STEPS

1. enable
2. configure terminal
3. aaa new-model
4. aaa authentication login default local
5. aaa authentication rejected \( n \) in \( m \) ban \( x \)
6. end
7. show aaa local user blocked
8. clear aaa local user blocked username \( \text{username} \)

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td>Example: Device(config)# aaa new-model</td>
<td>Enables the authentication, authorization, and accounting (AAA) access control model.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa authentication login default local</td>
</tr>
<tr>
<td>Example: Device(config)# aaa authentication login default local</td>
<td>Sets the authentication, authorization, and accounting (AAA) authentication by using the default authentication methods.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>aaa authentication rejected ( n ) in ( m ) ban ( x )</td>
</tr>
<tr>
<td>Example: Device(config)# aaa authentication rejected 3 in 20 ban 300</td>
<td>Configures the time period for which an user is blocked, if the user fails to successfully login within the specified time and login attempts.</td>
</tr>
<tr>
<td></td>
<td>• ( n )—Specifies the number of times a user can try to login.</td>
</tr>
<tr>
<td></td>
<td>• ( m )— Specifies the number of seconds within which an user can try to login.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• x—Specifies the time period an user is banned if the user fails to successfully login.</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 6

- **end**
  - **Example:**
    - Device(config)# end

  Exits global configuration mode and returns to privileged EXEC mode.

#### Step 7

- **show aaa local user blocked**
  - **Example:**
    - Device# show aaa local user blocked

  Displays the list of local users who were blocked.

#### Step 8

- **clear aaa local user blocked username username**
  - **Example:**
    - Device# clear aaa local user blocked username user1

  Clears the information about the blocked local user.

---

**Example**

The following is sample output from the **show aaa local user blocked** command:

```
Device# show aaa local user blocked

Local-user       State
user1            Watched (till 11:34:42 IST Feb 5 2015)
```

---

### Configuring VLAN ID-based MAC Authentication

Beginning in privileged EXEC mode, follow these steps:

#### SUMMARY STEPS

1. configure terminal
2. mab request format attribute 32 vlan access-vlan
3. copy running-config startup-config

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Open1x

Beginning in privileged EXEC mode, follow these steps to enable manual control of the port authorization state:

#### SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. switchport mode access
4. authentication control-direction {both | in}
5. authentication fallback name
6. authentication host-mode [multi-auth | multi-domain | multi-host | single-host]
7. authentication open
8. authentication order [ dot1x | mab ] [ webauth ]
9. authentication periodic
10. authentication port-control { auto | force-authorized | force-un authorized }
11. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td>switchport mode access</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Configures the port control as unidirectional or bidirectional.</td>
</tr>
<tr>
<td>authentication control-direction</td>
<td>{both</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication control-direction both</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Configures a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.</td>
</tr>
<tr>
<td>authentication fallback name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication fallback profile1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Sets the authorization manager mode on a port.</td>
</tr>
<tr>
<td>authentication host-mode</td>
<td>[multi-auth</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication host-mode multi-auth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Enables or disable open access on a port.</td>
</tr>
<tr>
<td>authentication open</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication open</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>(Optional) Sets the order of authentication methods used on a port.</td>
</tr>
<tr>
<td>authentication order</td>
<td>[dot1x</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication order dot1x webauth</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>(Optional) Enables or disable reauthentication on a port.</td>
</tr>
<tr>
<td>authentication periodic</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication periodic</td>
<td></td>
</tr>
</tbody>
</table>
Disabling 802.1x Authentication on the Port

You can disable 802.1x authentication on the port by using the `no dot1x pae` interface configuration command. Beginning in privileged EXEC mode, follow these steps to disable 802.1x authentication on the port. This procedure is optional.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `switchport mode access`
4. `no dot1x pae authenticator`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
</tbody>
</table>
### Resetting the 802.1x Authentication Configuration to the Default Values

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x authentication configuration to the default values. This procedure is optional.

#### SUMMARY STEPS

1. ```configure terminal```
2. ```interface interface-id```
3. ```dot1x default```
4. ```end```

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch#$ configure terminal</code>&lt;br&gt;Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config)# interface gigabitethernet 0/2</code>&lt;br&gt;Enters interface configuration mode, and specify the port to be configured.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Purpose**

**Step 3**

**dot1x default**

*Example:*

```
Switch(config-if)# dot1x default
```

- Resets the 802.1x parameters to the default values.

**Step 4**

**end**

*Example:*

```
Switch(config-if)# end
```

- Returns to privileged EXEC mode.

---

## Monitoring 802.1x Statistics and Status

*Table 87: Privileged EXEC show Commands*

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show dot1x all statistics</code></td>
<td>Displays 802.1x statistics for all ports</td>
</tr>
<tr>
<td><code>show dot1x interface interface-id statistics</code></td>
<td>Displays 802.1x statistics for a specific port</td>
</tr>
<tr>
<td>`show dot1x all [count</td>
<td>details</td>
</tr>
<tr>
<td><code>show dot1x interface interface-id</code></td>
<td>Displays the 802.1x administrative and operational status for a specific port</td>
</tr>
</tbody>
</table>

*Table 88: Global Configuration Commands*

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no dot1x logging verbose</code></td>
<td>Filters verbose 802.1x authentication messages (beginning with Cisco IOS Release 12.2(55)SE)</td>
</tr>
</tbody>
</table>

For detailed information about the fields in these displays, see the command reference for this release.
Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature Information for 802.1x Port-Based Authentication

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>Supports the use of same authorization methods on all the Catalyst switches in a network.</td>
</tr>
<tr>
<td></td>
<td>Supports filtering verbose system messages from the authentication manager.</td>
</tr>
</tbody>
</table>
Configuring Port-Based Traffic Control

- Overview of Port-Based Traffic Control, on page 864
- Finding Feature Information, on page 864
- Information About Storm Control, on page 864
- How to Configure Storm Control, on page 866
- Finding Feature Information, on page 873
- Information About Protected Ports, on page 873
- How to Configure Protected Ports, on page 874
- Monitoring Protected Ports, on page 876
- Where to Go Next, on page 876
- Additional References, on page 876
- Feature Information, on page 877
- Finding Feature Information, on page 877
- Information About Port Blocking, on page 877
- How to Configure Port Blocking, on page 878
- Monitoring Port Blocking, on page 879
- Where to Go Next, on page 880
- Additional References, on page 880
- Feature Information, on page 881
- Prerequisites for Port Security, on page 881
- Restrictions for Port Security, on page 881
- Information About Port Security, on page 881
- How to Configure Port Security, on page 886
- Configuration Examples for Port Security, on page 893
- Additional References, on page 894
- Finding Feature Information, on page 894
- Information About Protocol Storm Protection, on page 895
- How to Configure Protocol Storm Protection, on page 895
- Monitoring Protocol Storm Protection, on page 897
- Additional References, on page 897
Overview of Port-Based Traffic Control

Port-based traffic control is a set of Layer 2 features on the Cisco Catalyst switches used to filter or block packets at the port level in response to specific traffic conditions. The following port-based traffic control features are supported in the Cisco IOS Release for which this guide is written:

- Storm Control
- Protected Ports
- Port Blocking
- Port Security
- Protocol Storm Protection

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Storm Control

Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

How Traffic Activity is Measured

Storm control uses one of these methods to measure traffic activity:

- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic
• Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received
• Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received
• Traffic rate in packets per second and for small frames. This feature is enabled globally. The threshold for small frames is configured for each interface.

With each method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold (if one is specified) and then resumes normal forwarding. If the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. In general, the higher the level, the less effective the protection against broadcast storms.

When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as OSPF, and regular multicast data traffic, so both types of traffic are blocked.

Traffic Patterns

Figure 58: Broadcast Storm Control Example

This example shows broadcast traffic patterns on an interface over a given period of time.

Broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

The combination of the storm-control suppression level and the 1-second time interval controls the way the storm control algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100 percent means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.
Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of storm control.

You use the `storm-control` interface configuration commands to set the threshold value for each traffic type.

---

**How to Configure Storm Control**

### Configuring Storm Control and Threshold Levels

You configure storm control on a port and enter the threshold level that you want to be used for a particular type of traffic.

However, because of hardware limitations and the way in which packets of different sizes are counted, threshold percentages are approximations. Depending on the sizes of the packets making up the incoming traffic, the actual enforced threshold might differ from the configured level by several percentage points.

---

**Note**

Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

Follow these steps to storm control and threshold levels:

**Before you begin**

Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

---

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}`
5. `storm-control action {shutdown | trap}`
6. `end`
7. `show storm-control [interface-id] [broadcast | multicast | unicast]`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**
**configure terminal**
**Example:**
Switch# configure terminal

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet1/0/1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures broadcast, multicast, or unicast storm control. By default, storm control is disabled.</td>
</tr>
<tr>
<td>storm-control {broadcast</td>
<td>By default, storm control is disabled.</td>
</tr>
<tr>
<td>multicast</td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td>unicast</td>
<td>• For level, specifies the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00.</td>
</tr>
<tr>
<td>level level-low</td>
<td>• (Optional) For level-low, specifies the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00.</td>
</tr>
<tr>
<td>[bps bps [bps-low]</td>
<td>If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked.</td>
</tr>
<tr>
<td>[pps pps [pps-low]]}</td>
<td>• For bps bps, specifies the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0.</td>
</tr>
<tr>
<td>Example:</td>
<td>• (Optional) For bps-low, specifies the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0.</td>
</tr>
<tr>
<td>Switch(config-if)# storm-control unicast level 87 65</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Storm Control and Threshold Levels

You configure storm control on a port and enter the threshold level that you want to be used for a particular type of traffic.

However, because of hardware limitations and the way in which packets of different sizes are counted, threshold percentages are approximations. Depending on the sizes of the packets making up the incoming traffic, the actual enforced threshold might differ from the configured level by several percentage points.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>for pps</strong>, specifies the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0.</td>
<td></td>
</tr>
<tr>
<td>(Optional) For pps-low, specifies the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0.</td>
<td></td>
</tr>
</tbody>
</table>

For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.

**Step 5**

storm-control action {shutdown | trap}

Example:

Switch(config-if)# storm-control action trap

Specifies the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps.

- Select the shutdown keyword to error-disable the port during a storm.
- Select the trap keyword to generate an SNMP trap when a storm is detected.

**Step 6**

end

Example:

Switch(config-if)# end

Returns to privileged EXEC mode.

**Step 7**

show storm-control [interface-id] [broadcast | multicast | unicast]

Example:

Switch# show storm-control gigabitethernet1/0/1 unicast

Verifies the storm control suppression levels set on the interface for the specified traffic type. If you do not enter a traffic type, details for all traffic types (broadcast, multicast and unicast) are displayed.

**Step 8**

copy running-config startup-config

Example:

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.
Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

Follow these steps to storm control and threshold levels:

**Before you begin**
Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **storm-control action {shutdown | trap}**
5. **storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}**
6. **end**
7. **show storm-control [interface-id] [broadcast | multicast | unicast]**
8. **copy running-config startup-config**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>2.</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><code>interface interface-id</code></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>`storm-control action {shutdown</td>
<td>trap}`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Storm Control and Threshold Levels

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config-if)# storm-control action trap | - Select the `shutdown` keyword to error-disable the port during a storm.  
- Select the `trap` keyword to generate an SNMP trap when a storm is detected. |

**Step 5**

```
storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}
```

**Example:**

```
Switch(config-if)# storm-control unicast level 87 65
```

Configures broadcast, multicast, or unicast storm control. By default, storm control is disabled.

The keywords have these meanings:

- For `level`, specifies the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00.

  - (Optional) For `level-low`, specifies the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00.

  - If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked.

- For `bps bps`, specifies the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0.

  - (Optional) For `bps-low`, specifies the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0.

- For `pps pps`, specifies the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0.

  - (Optional) For `pps-low`, specifies the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is **0.0 to 10000000000.0**.
### Configuring Small-Frame Arrival Rate

Incoming VLAN-tagged packets smaller than 67 bytes are considered small frames. They are forwarded by the switch, but they do not cause the switch storm-control counters to increment.

You globally enable the small-frame arrival feature on the switch and then configure the small-frame threshold for packets on each interface. Packets smaller than the minimum size and arriving at a specified rate (the threshold) are dropped since the port is error disabled.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. errdisable detect cause small-frame
4. errdisable recovery interval *interval*
5. errdisable recovery cause small-frame
6. interface *interface-id*
7. small-frame violation-rate *pps*
8. end
9. show interfaces *interface-id*
10. show running-config
11. copy running-config startup-config

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring Small-Frame Arrival Rate

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables the small-frame rate-arrival feature on the switch.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Specifies the time to recover from the specified error-disabled state.</td>
</tr>
<tr>
<td><code>errdisable detect cause small-frame</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# errdisable detect cause small-frame</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Configures the recovery time for error-disabled ports to be automatically re-enabled after they are error disabled by the arrival of small frames. Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.</td>
</tr>
<tr>
<td><code>errdisable recovery interval interval</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# errdisable recovery interval 60</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the threshold rate for the interface to drop incoming packets and error disable the port. The range is 1 to 10,000 packets per second (pps).</td>
</tr>
<tr>
<td><code>errdisable recovery cause small-frame</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# errdisable recovery cause small-frame</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Enters interface configuration mode, and specify the interface to be configured.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet1/0/2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>small-frame violation-rate pps</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# small-frame violation rate 10000</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [http://www.cisco.com/go/efi](http://www.cisco.com/go/efi). An account on Cisco.com is not required.

### Information About Protected Ports

#### Protected Ports

Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbor does not see the traffic generated by another neighbor. In such an environment, the use of protected ports ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch.

Protected ports have these features:

- A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control
traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.

- Forwarding behavior between a protected port and a nonprotected port proceeds as usual.

Because a switch stack represents a single logical switch, Layer 2 traffic is not forwarded between any protected ports in the switch stack, whether they are on the same or different switches in the stack.

Default Protected Port Configuration

The default is to have no protected ports defined.

Protected Ports Guidelines

You can configure protected ports on a physical interface (for example, Gigabit Ethernet port 1) or an EtherChannel group (for example, port-channel 5). When you enable protected ports for a port channel, it is enabled for all ports in the port-channel group.

How to Configure Protected Ports

Configuring a Protected Port

Before you begin

Protected ports are not pre-defined. This is the task to configure one.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. switchport protected
5. end
6. show interfaces interface-id switchport
7. show running-config
8. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport protected</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# switchport protected</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# show interfaces gigabitethernet 0/1 switchport</td>
</tr>
<tr>
<td>Step 7</td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>
Monitoring Protected Ports

Table 89: Commands for Displaying Protected Port Settings

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.</td>
</tr>
</tbody>
</table>

Where to Go Next

Additional References

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature Information

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Port Blocking

Port Blocking

By default, the switch floods packets with unknown destination MAC addresses out of all ports. If unknown unicast and multicast traffic is forwarded to a protected port, there could be security issues. To prevent unknown unicast or multicast traffic from being forwarded from one port to another, you can block a port (protected or nonprotected) from flooding unknown unicast or multicast packets to other ports.
# How to Configure Port Blocking

## Blocking Flooded Traffic on an Interface

**Before you begin**

The interface can be a physical interface or an EtherChannel group. When you block multicast or unicast traffic for a port channel, it is blocked on all ports in the port-channel group.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `switchport block multicast`
5. `switchport block unicast`
6. `end`
7. `show interfaces interface-id switchport`
8. `show running-config`
9. `copy running-config startup-config`

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> <code>Switch&gt; enable</code></td>
<td><em>Example:</em> <code>Switch&gt; enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> <code>Switch# configure terminal</code></td>
<td><em>Example:</em> <code>Switch# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> <code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td><em>Example:</em> <code>Switch(config)# interface gigabitethernet 0/1</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Blocks unknown multicast forwarding out of the port.</td>
</tr>
<tr>
<td><code>switchport block multicast</code></td>
<td>Blocks unknown multicast forwarding out of the port.</td>
</tr>
<tr>
<td><em>Note</em></td>
<td>Pure Layer 2 multicast traffic as well as multicast packets that contain IPv6 information in the header are blocked.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td><em>Example:</em></td>
</tr>
</tbody>
</table>
### Monitoring Port Blocking

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-if)# switchport block multicast</code></td>
<td>Blocks unknown multicast forwarding out of the port.</td>
</tr>
</tbody>
</table>

**Step 5**

**switchport block unicast**

**Example:**

`Switch(config-if)# switchport block unicast`

**Step 6**

**end**

**Example:**

`Switch(config)# end`

**Step 7**

**show interfaces interface-id switchport**

**Example:**

`Switch# show interfaces gigabitethernet 0/1 switchport`

**Step 8**

**show running-config**

**Example:**

`Switch# show running-config`

**Step 9**

**copy running-config startup-config**

**Example:**

`Switch# copy running-config startup-config`

---

**Table 90: Commands for Displaying Port Blocking Settings**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id] switchport</code></td>
<td>Displays the administrative and operational status of all switching (nonrouting) ports or the specified port, including port blocking and port protection settings.</td>
</tr>
</tbody>
</table>
Where to Go Next

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature Information

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EXCisco IOS Release</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisites for Port Security

**Note**

If you try to set the maximum value to a number less than the number of secure addresses already configured on an interface, the command is rejected.

Restrictions for Port Security

The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system. This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

Information About Port Security

Port Security

You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.

Related Topics

- Enabling and Configuring Port Security
- Configuration Examples for Port Security, on page 893
Types of Secure MAC Addresses

The switch supports these types of secure MAC addresses:

- Static secure MAC addresses—These are manually configured by using the `switchport port-security mac-address mac-address` interface configuration command, stored in the address table, and added to the switch running configuration.

- Dynamic secure MAC addresses—These are dynamically configured, stored only in the address table, and removed when the switch restarts.

- Sticky secure MAC addresses—These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.

Sticky Secure MAC Addresses

You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. The interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses. All sticky secure MAC addresses are added to the running configuration.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If you save the sticky secure MAC addresses in the configuration file, when the switch restarts, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost.

If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.

- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

- Running diagnostic tests with port security enabled.

You can configure the interface for one of three violation modes, based on the action to be taken if a violation occurs:

- `protect`—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.
We do not recommend configuring the protect violation mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- **restrict**—when the number of secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- **shutdown**—a port security violation causes the interface to become error-disabled and to shut down immediately, and the port LED turns off. When a secure port is in the error-disabled state, you can bring it out of this state by entering the `errdisable recovery cause psecure-violation` global configuration command, or you can manually re-enable it by entering the `shutdown` and `no shut down` interface configuration commands. This is the default mode.

- **shutdown vlan**—Use to set the security violation mode per-VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs.

This table shows the violation mode and the actions taken when you configure an interface for port security.

**Table 91: Security Violation Mode Actions**

<table>
<thead>
<tr>
<th>Violation Mode</th>
<th>Traffic is forwarded</th>
<th>Sends SNMP trap</th>
<th>Sends syslog message</th>
<th>Displays error message</th>
<th>Violation counter increments</th>
<th>Shuts down port</th>
</tr>
</thead>
<tbody>
<tr>
<td>protect</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>restrict</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>shutdown</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>shutdown vlan</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

11 Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
12 The switch returns an error message if you manually configure an address that would cause a security violation.
13 Shuts down only the VLAN on which the violation occurred.

**Port Security Aging**

You can use port security aging to set the aging time for all secure addresses on a port. Two types of aging are supported per port:

- **Absolute**—The secure addresses on the port are deleted after the specified aging time.
• Inactivity—The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Related Topics

Enabling and Configuring Port Security Aging, on page 891

Default Port Security Configuration

Table 92: Default Port Security Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port security</td>
<td>Disabled on a port.</td>
</tr>
<tr>
<td>Sticky address learning</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Maximum number of secure MAC addresses per port</td>
<td>1.</td>
</tr>
<tr>
<td>Violation mode</td>
<td>Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.</td>
</tr>
<tr>
<td>Port security aging</td>
<td>Disabled. Aging time is 0.</td>
</tr>
<tr>
<td></td>
<td>Static aging is disabled.</td>
</tr>
<tr>
<td></td>
<td>Type is absolute.</td>
</tr>
</tbody>
</table>

Port Security Configuration Guidelines

• Port security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.

• A secure port cannot be a destination port for Switched Port Analyzer (SPAN).

  
  Note
  Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.

• When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the phone.

• When a trunk port configured with port security and assigned to an access VLAN for data traffic and to a voice VLAN for voice traffic, entering the `switchport voice` and `switchport priority extend` interface configuration commands has no effect.

  When a connected device uses the same MAC address to request an IP address for the access VLAN and then an IP address for the voice VLAN, only the access VLAN is assigned an IP address.
- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

- The switch does not support port security aging of sticky secure MAC addresses.

This table summarizes port security compatibility with other port-based features.

**Table 93: Port Security Compatibility with Other Switch Features**

<table>
<thead>
<tr>
<th>Type of Port or Feature on Port</th>
<th>Compatible with Port Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTP port</td>
<td>No</td>
</tr>
<tr>
<td>Trunk port</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic-access port</td>
<td>No</td>
</tr>
<tr>
<td>Routed port</td>
<td>No</td>
</tr>
<tr>
<td>SPAN source port</td>
<td>Yes</td>
</tr>
<tr>
<td>SPAN destination port</td>
<td>No</td>
</tr>
<tr>
<td>EtherChannel</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunneling port</td>
<td>Yes</td>
</tr>
<tr>
<td>Protected port</td>
<td>Yes</td>
</tr>
<tr>
<td>IEEE 802.1x port</td>
<td>Yes</td>
</tr>
<tr>
<td>Voice VLAN port</td>
<td>Yes</td>
</tr>
<tr>
<td>IP source guard</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic Address Resolution Protocol (ARP) inspection</td>
<td>Yes</td>
</tr>
<tr>
<td>Flex Links</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

14 DTP=Dynamic Trunking Protocol  
15 A port configured with the `switchport mode dynamic` interface configuration command.  
16 A VLAN Query Protocol (VQP) port configured with the `switchport access vlan dynamic` interface configuration command.  
17 You must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN.
How to Configure Port Security

Enabling and Configuring Port Security

Before you begin

This task restricts input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

SUMMARY STEPS

1. enable
2. configure terminal
3. port-security mac-address forbidden mac address
4. interface interface-id
5. switchport mode {access | trunk}
6. switchport voice vlan vlan-id
7. switchport port-security
8. switchport port-security [maximum value [vlan {vlan-list | {access | voice}}]]
9. switchport port-security violation {protect | restrict | shutdown | shutdown vlan}
10. switchport port-security [mac-address mac-address [vlan {vlan-id | {access | voice}}]]
11. switchport port-security mac-address sticky
12. switchport port-security mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}]
13. switchport port-security mac-address forbidden mac address
14. end
15. show port-security
16. show running-config
17. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>port-security mac-address forbidden</code> <em>mac address</em></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# port-security mac-address forbidden 2.2.2</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>interface</code> <em>interface-id</em></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config)# interface gigabitethernet 0/1</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>switchport mode</code> {access</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-if)# switchport mode access</code></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>switchport voice vlan</code> <em>vlan-id</em></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-if)# switchport voice vlan 22</code></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>switchport port-security</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-if)# switchport port-security</code></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>switchport port-security [maximum value</code> <em>vlan</em></td>
</tr>
<tr>
<td>Example:</td>
<td>`{vlan-list</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-if)# switchport port-security maximum 20</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
- `Switch(config)#` and `Switch(config-if)#` are used to indicate the configuration prompt for the switch.
- `Switch(config-if)#` is used for interface configuration.
- `Switch(config)#` is used for global configuration.

---

**Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)**
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• access — On an access port, specifies the VLAN as an access VLAN.</td>
<td></td>
</tr>
<tr>
<td>• voice — On an access port, specifies the VLAN as a voice VLAN.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** The voice keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.

### Step 9

**switchport port-security violation** \{protect \| restrict \| shutdown \| shutdown vlan\}

**Example:**

```plaintext
Switch(config-if)# switchport port-security violation restrict
```

(Optional) Sets the violation mode, the action to be taken when a security violation is detected, as one of these:

- **protect** — When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

**Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- **restrict** — When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- **shutdown** — The interface is error-disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- **shutdown vlan** — Use to set the security violation mode per VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>Note</strong> When a secure port is in the error-disabled state, you can bring it out of this state by entering the <code>errdisable recovery cause psecure-violation</code> global configuration command. You can manually re-enable it by entering the <code>shutdown</code> and <code>no shutdown</code> interface configuration commands or by using the <code>clear errdisable interface vlan</code> privileged EXEC command.</td>
</tr>
<tr>
<td>`switchport port-security [mac-address mac-address [vlan {vlan-id</td>
<td>{access</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Note If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration.</td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice</code></td>
<td>(Optional) <code>vlan</code>—sets a per-VLAN maximum value. Enter one of these options after you enter the <code>vlan</code> keyword:</td>
</tr>
<tr>
<td></td>
<td>• <code>vlan-id</code>—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used.</td>
</tr>
<tr>
<td></td>
<td>• <code>access</code>—On an access port, specifies the VLAN as an access VLAN.</td>
</tr>
<tr>
<td></td>
<td>• <code>voice</code>—On an access port, specifies the VLAN as a voice VLAN.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Note The <code>voice</code> keyword is available only if a voice VLAN is configured on a port and if that port is not the access VLAN. If an interface is configured for voice VLAN, configure a maximum of two secure MAC addresses.</td>
</tr>
<tr>
<td><code>switchport port-security mac-address sticky</code></td>
<td>(Optional) Enables sticky learning on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport port-security mac-address sticky</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>switchport port-security mac-address sticky</strong>&lt;br&gt;**[mac-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Enters a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, and are converted to sticky secure MAC addresses, and are added to the running configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address.</td>
</tr>
<tr>
<td></td>
<td>(Optional) <strong>vlan</strong>—sets a per-VLAN maximum value.</td>
</tr>
<tr>
<td></td>
<td>Enter one of these options after you enter the <strong>vlan</strong> keyword:</td>
</tr>
<tr>
<td></td>
<td>• <strong>vlan-id</strong>—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>access</strong>—On an access port, specifies the VLAN as an access VLAN.</td>
</tr>
<tr>
<td></td>
<td>• <strong>voice</strong>—On an access port, specifies the VLAN as a voice VLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The <strong>voice</strong> keyword is available only if a voice VLAN is configured on a port and that port is not the access VLAN.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>switchport port-security mac-address forbidden</strong> <strong>mac address</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies a MAC address that should be forbidden by port-security on the particular interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Switch(config-if)# switchport port-security</strong>&lt;br&gt;<strong>mac-address forbidden 2.2.2</strong></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Switch(config)# end</strong></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>show port-security</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td><strong>Switch# show port-security</strong></td>
</tr>
</tbody>
</table>
Enabling and Configuring Port Security Aging

Use this feature to remove and add devices on a secure port without manually deleting the existing secure MAC addresses and to still limit the number of secure addresses on a port. You can enable or disable the aging of secure addresses on a per-port basis.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. switchport port-security aging {static | time time | type {absolute | inactivity}}
5. end
6. show port-security [interface interface-id] [address]
7. show running-config
8. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Enabling and Configuring Port Security Aging

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4 switchport port-security aging  {static</td>
<td>time time</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: The switch does not support port security aging of sticky secure addresses.</td>
</tr>
<tr>
<td>Switch(config-if)# switchport port-security aging time 120</td>
<td>Enter static to enable aging for statically configured secure addresses on this port.</td>
</tr>
<tr>
<td></td>
<td>For time, specifies the aging time for this port. The valid range is from 0 to 1440 minutes.</td>
</tr>
<tr>
<td></td>
<td>For type, select one of these keywords:</td>
</tr>
<tr>
<td></td>
<td>• absolute—Sets the aging type as absolute aging. All the secure addresses on this port</td>
</tr>
<tr>
<td></td>
<td>age out exactly after the time (minutes) specified lapses and are removed from the</td>
</tr>
<tr>
<td></td>
<td>secure address list.</td>
</tr>
<tr>
<td></td>
<td>• inactivity—Sets the aging type as inactivity aging. The secure addresses on this port</td>
</tr>
<tr>
<td></td>
<td>age out only if there is no data traffic from the secure source addresses for the specified time period.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6 show port-security [interface interface-id] [address]</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show port-security interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Step 7 show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Related Topics
Port Security Aging, on page 883

Configuration Examples for Port Security

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 50. The violation mode is the default, no static secure MAC addresses are configured, and sticky learning is enabled.

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 50
Switch(config-if)# switchport port-security mac-address sticky
```

This example shows how to configure a static secure MAC address on VLAN 3 on a port:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

This example shows how to enable sticky port security on a port, to manually configure MAC addresses for data VLAN and voice VLAN, and to set the total maximum number of secure addresses to 20 (10 for data VLAN and 10 for voice VLAN).

```
Switch(config)# interface tengigabitethernet 0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

Related Topics
Port Security, on page 881
Enabling and Configuring Port Security
Additional References

Error Message Decoder

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Information About Protocol Storm Protection

Protocol Storm Protection

When a switch is flooded with Address Resolution Protocol (ARP) or control packets, high CPU utilization can cause the CPU to overload. These issues can occur:

- Routing protocol can flap because the protocol control packets are not received, and neighboring adjacencies are dropped.
- Spanning Tree Protocol (STP) reconverges because the STP bridge protocol data unit (BPDU) cannot be sent or received.
- CLI is slow or unresponsive.

Using protocol storm protection, you can control the rate at which control packets are sent to the switch by specifying the upper threshold for the packet flow rate. The supported protocols are ARP, ARP snooping, Dynamic Host Configuration Protocol (DHCP) v4, DHCP snooping, Internet Group Management Protocol (IGMP), and IGMP snooping.

When the packet rate exceeds the defined threshold, the switch drops all traffic arriving on the specified virtual port for 30 seconds. The packet rate is measured again, and protocol storm protection is again applied if necessary.

For further protection, you can manually error disable the virtual port, blocking all incoming traffic on the virtual port. You can manually enable the virtual port or set a time interval for automatic re-enabling of the virtual port.

Excess packets are dropped on no more than two virtual ports.

Virtual port error disabling is not supported for EtherChannel and Flexlink interfaces.

Default Protocol Storm Protection Configuration

Protocol storm protection is disabled by default. When it is enabled, auto-recovery of the virtual port is disabled by default.

How to Configure Protocol Storm Protection

Enabling Protocol Storm Protection

SUMMARY STEPS

1. enable
2. configure terminal
3. psp {arp | dhcp | igmp} pps value
4. `errdisable detect cause psp`
5. `errdisable recovery interval time`
6. `end`
7. `show psp config {arp | dhcp | igmp}`

## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch&gt; <code>enable</code></td>
<td><code>• Enter your password if prompted.</code></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> psp `{arp</td>
<td>dhcp</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# <code>psp dhcp pps 35</code></td>
<td>For <em>value</em>, specifies the threshold value for the number of packets per second. If the traffic exceeds this value, protocol storm protection is enforced. The range is from 5 to 50 packets per second.</td>
</tr>
<tr>
<td><strong>Step 4</strong> errdisable detect cause psp</td>
<td>(Optional) Enables error-disable detection for protocol storm protection. If this feature is enabled, the virtual port is error disabled. If this feature is disabled, the port drops excess packets without error disabling the port.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# <code>errdisable detect cause psp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> errdisable recovery interval <em>time</em></td>
<td>(Optional) Configures an auto-recovery time (in seconds) for error-disabled virtual ports. When a virtual port is error-disabled, the switch auto-recons after this time. The range is from 30 to 86400 seconds.</td>
</tr>
<tr>
<td><em>Example:</em> Switch</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show psp config `{arp</td>
<td>dhcp</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring Protocol Storm Protection

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show psp config {arp</td>
<td>dhcp</td>
</tr>
</tbody>
</table>

### Additional References

**Error Message Decoder**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help you research and resolve system error messages in this release, use the Error Message Decoder tool.</td>
<td><a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a></td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
PART X

System Management

• Administering the System, on page 901
• Performing Switch Setup Configuration, on page 935
• Configuring System Message Logs, on page 965
• Configuring Online Diagnostics, on page 979
• Troubleshooting the Software Configuration, on page 989
Administering the System

Information About Administering the Switch

System Time and Date Management

You can manage the system time and date on your switch using automatic configuration methods (RTC and NTP), or manual configuration methods.

Note

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Configuration Fundamentals Command Reference on Cisco.com.

System Clock

The basis of the time service is the system clock. This clock runs from the moment the system starts up and keeps track of the date and time.

The system clock can then be set from these sources:

- RTC
- NTP
- Manual configuration

The system clock can provide time to these services:

- User show commands
• Logging and debugging messages

The system clock keeps track of time internally based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). You can configure information about the local time zone and summer time (daylight saving time) so that the time appears correctly for the local time zone.

The system clock keeps track of whether the time is authoritative or not (that is, whether it has been set by a time source considered to be authoritative). If it is not authoritative, the time is available only for display purposes and is not redistributed.

Real Time Clock

A real-time clock (RTC) keeps track of the current time on the switch. The switch is shipped to you with RTC set to GMT time until you reconfigure clocking parameters.

The benefits of an RTC are:
• RTC is battery-powered.
• System time is retained during power outage and at system reboot.

The RTC and NTP clocks are integrated on the switch. When NTP is enabled, the RTC time is periodically synchronized to the NTP clock to maintain accuracy.

Network Time Protocol

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

NTP uses the concept of a stratum to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.

The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.
Cisco’s implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

The Figure shows a typical network example using NTP. Switch A is the NTP master, with the Switch B, C, and D configured in NTP server mode, in server association with Switch A. Switch E is configured as an NTP peer to the upstream and downstream Switch, Switch B and Switch F, respectively.

Figure 59: Typical NTP Network Configuration

If the network is isolated from the Internet, Cisco’s implementation of NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

### NTP Stratum

NTP uses the concept of a *stratum* to describe how many NTP hops away a device is from an authoritative time source. A stratum 1 time server has a radio or atomic clock directly attached, a stratum 2 time server receives its time through NTP from a stratum 1 time server, and so on. A device running NTP automatically chooses as its time source the device with the lowest stratum number with which it communicates through NTP. This strategy effectively builds a self-organizing tree of NTP speakers.

NTP avoids synchronizing to a device whose time might not be accurate by never synchronizing to a device that is not synchronized. NTP also compares the time reported by several devices and does not synchronize to a device whose time is significantly different than the others, even if its stratum is lower.
NTP Associations

The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

NTP Security

The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

NTP Implementation

Implementation of NTP does not support stratum 1 service; it is not possible to connect to a radio or atomic clock. We recommend that the time service for your network be derived from the public NTP servers available on the IP Internet.

Figure 60: Typical NTP Network Configuration

The following figure shows a typical network example using NTP. Switch A is the NTP master, with the Switch B, C, and D configured in NTP server mode, in server association with Switch A. Switch E is configured as an NTP peer to the upstream and downstream switches, Switch B and Switch F.
If the network is isolated from the Internet, NTP allows a device to act as if it is synchronized through NTP, when in fact it has learned the time by using other means. Other devices then synchronize to that device through NTP.

When multiple sources of time are available, NTP is always considered to be more authoritative. NTP time overrides the time set by any other method.

Several manufacturers include NTP software for their host systems, and a publicly available version for systems running UNIX and its various derivatives is also available. This software allows host systems to be time-synchronized as well.

**NTP Version 4**

NTP version 4 is implemented on the switch. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Support for IPv6.
- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

For details about configuring NTPv4, see the Implementing NTPv4 in IPv6 chapter of the *Cisco IOS IPv6 Configuration Guide, Release 12.4T*.

**System Name and Prompt**

You configure the system name on the Switch to identify it. By default, the system name and prompt are Switch.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol [>] is appended. The prompt is updated whenever the system name changes.

For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*.

**Stack System Name and Prompt**

If you are accessing a stack member through the active switch, you must use the session stack-member-number privileged EXEC command. The stack member number range is from 1 through 8. When you use this command, the stack member number is appended to the system prompt. For example, Switch-2# is the prompt in privileged EXEC mode for stack member 2, and the system prompt for the switch stack is Switch.

**Default System Name and Prompt Configuration**

The default switch system name and prompt is *Switch*. 
The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map hostnames to IP addresses. When you configure DNS on your switch, you can substitute the hostname for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, for example, the File Transfer Protocol (FTP) system is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, specify the name server that is present on your network, and enable the DNS.

### Default DNS Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS enable state</td>
<td>Enabled.</td>
</tr>
<tr>
<td>DNS default domain name</td>
<td>None configured.</td>
</tr>
<tr>
<td>DNS servers</td>
<td>No name server addresses are configured.</td>
</tr>
</tbody>
</table>

### Login Banners

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner is displayed on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner is also displayed on all connected terminals. It appears after the MOTD banner and before the login prompts.

---

**Note**

For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.4*.

### Default Banner Configuration

The MOTD and login banners are not configured.

### MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- **Dynamic address**—A source MAC address that the switch learns and then ages when it is not in use.
• Static address—A manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

Note
For complete syntax and usage information for the commands used in this section, see the command reference for this release.

MAC Address Table Creation

With multiple MAC addresses supported on all ports, you can connect any port on the switch to other network devices. The switch provides dynamic addressing by learning the source address of packets it receives on each port and adding the address and its associated port number to the address table. As devices are added or removed from the network, the switch updates the address table, adding new dynamic addresses and aging out those that are not in use.

The aging interval is globally configured. However, the switch maintains an address table for each VLAN, and STP can accelerate the aging interval on a per-VLAN basis.

The switch sends packets between any combination of ports, based on the destination address of the received packet. Using the MAC address table, the switch forwards the packet only to the port associated with the destination address. If the destination address is on the port that sent the packet, the packet is filtered and not forwarded. The switch always uses the store-and-forward method: complete packets are stored and checked for errors before transmission.

MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Unicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 1 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

Default MAC Address Table Settings

The following table shows the default settings for the MAC address table.

Table 95: Default Settings for the MAC Address

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aging time</td>
<td>300 seconds</td>
</tr>
<tr>
<td>Dynamic addresses</td>
<td>Automatically learned</td>
</tr>
<tr>
<td>Static addresses</td>
<td>None configured</td>
</tr>
</tbody>
</table>
ARP Table Management

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning the local data link address from an IP address is called address resolution.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the arpa keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

For CLI procedures, see the Cisco IOS Release 12.4 documentation on Cisco.com.

How to Administer the Switch

Configuring the Time and Date Manually

System time remains accurate through restarts and reboot, however, you can manually configure the time and date after the system is restarted.

We recommend that you use manual configuration only when necessary. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

Note

You must reconfigure this setting if you have manually configured the system clock before the active switch fails and a different stack member assumes the role of active switch.

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Follow these steps to set the system clock:

SUMMARY STEPS

1. enable
2. Use one of the following:
   • clock set hh:mm:ss day month year
   • clock set hh:mm:ss month day year
## Configuring the Time Zone

Follow these steps to manually configure the time zone:

### SUMMARY STEPS

1. enable
2. configure terminal
3. clock timezone zone hours-offset [minutes-offset]
4. end
5. show running-config
6. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> clock set hh:mm:ss day month year</td>
<td>Manually set the system clock using one of these formats:</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# clock set 13:32:00 23 March 2013</td>
<td>• <em>hh:mm:ss</em>—Specifies the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone.</td>
</tr>
<tr>
<td></td>
<td>• <em>day</em>—Specifies the day by date in the month.</td>
</tr>
<tr>
<td></td>
<td>• <em>month</em>—Specifies the month by name.</td>
</tr>
<tr>
<td></td>
<td>• <em>year</em>—Specifies the year (no abbreviation).</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Internal time is kept in Coordinated Universal Time (UTC), so this command is used only for display purposes and when the time is manually set.</td>
</tr>
</tbody>
</table>
| `Switch(config)# clock timezone AST -3 30` | • `zone`—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC.  
• `hours-offset`—Enters the hours offset from UTC.  
• (Optional) `minutes-offset`—Enters the minutes offset from UTC. This available where the local time zone is a percentage of an hour different from UTC. |

**Step 4**

Example:  
`Switch(config)# end`

Returns to privileged EXEC mode.

**Step 5**

Example:  
`Switch# show running-config`

Verifies your entries.

**Step 6**

Example:  
`Switch# copy running-config startup-config`

(Optional) Saves your entries in the configuration file.

---

**Configuring Summer Time (Daylight Saving Time)**

To configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year, perform this task:

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. `clock summer-time zone date date month year hh:mm date month year hh:mm [offset]`  
4. `clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]`  
5. end  
6. `show running-config`  
7. `copy running-config startup-config`
# System Management

## Configuring Summer Time (Daylight Saving Time)

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; <code>enable</code></td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures summer time to start and end on specified days every year.</td>
</tr>
<tr>
<td><code>clock summer-time zone date date month year hh:mm date month year hh:mm [offset]]</code></td>
<td>Configures summer time to start and end on specified days every year.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures summer time to start and end on the specified days every year. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. Summer time is disabled by default. If you specify <code>clock summer-time zone recurring</code> without parameters, the summer time rules default to the United States rules. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.</td>
</tr>
<tr>
<td><code>clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]</code></td>
<td>Configures summer time to start and end on the specified days every year. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. Summer time is disabled by default. If you specify <code>clock summer-time zone recurring</code> without parameters, the summer time rules default to the United States rules. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00</code></td>
<td></td>
</tr>
</tbody>
</table>

- `zone`—Specifies the name of the time zone (for example, PDT) to be displayed when summer time is in effect.
- (Optional) `week`—Specifies the week of the month (1 to 4, `first`, or `last`).
- (Optional) `day`—Specifies the day of the week (Sunday, Monday...).
- (Optional) `month`—Specifies the month (January, February...).
- (Optional) `hh:mm`—Specifies the time (24-hour format) in hours and minutes.
- (Optional) `offset`—Specifies the number of minutes to add during summer time. The default is 60.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 5  
  end  
  Example:  
  Switch(config)# end | Returns to privileged EXEC mode. |
| Step 6  
  show running-config  
  Example:  
  Switch# show running-config | Verifies your entries. |
| Step 7  
  copy running-config startup-config  
  Example:  
  Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

Follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. clock summer-time zone date month date year hh:mm month date year hh:mm [offset] or clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]  
4. end  
5. show running-config  
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1  
  enable  
  Example:  
  Switch> enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| Step 2  
  configure terminal  
  Example:  
  Switch# configure terminal | Enters global configuration mode. |
Configuring a System Name

Follow these steps to manually configure a system name:

**SUMMARY STEPS**

1. enable
2. configure terminal

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 3    | `clock summer-time zone date [month date year hh:mm]` or `clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]` | Configures summer time to start on the first date and end on the second date. Summer time is disabled by default.  
   - For `zone`, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.  
   - (Optional) For `week`, specify the week of the month (1 to 5 or last).  
   - (Optional) For `day`, specify the day of the week (Sunday, Monday...).  
   - (Optional) For `month`, specify the month (January, February...).  
   - (Optional) For `hh:mm`, specify the time (24-hour format) in hours and minutes.  
   - (Optional) For `offset`, specify the number of minutes to add during summer time. The default is 60. |
| 4    | `end` | Returns to privileged EXEC mode. |
|      | **Example:**  
|      | `Switch(config)# end` |  |
| 5    | `show running-config` | Verifies your entries. |
|      | **Example:**  
|      | `Switch# show running-config` |  |
| 6    | `copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
|      | **Example:**  
|      | `Switch# copy running-config startup-config` |  |
3. `hostname name`
4. `end`
5. `show running-config`
6. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>hostname name</code></td>
<td>Configures a system name. When you set the system name, it is also used as the system prompt.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# hostname remote-users</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Setting Up DNS

If you use the switch IP address as its hostname, the IP address is used and no DNS query occurs. If you configure a hostname that contains no periods (.), a period followed by the default domain name is appended to the hostname before the DNS query is made to map the name to an IP address. The default domain name is the value set by the `ip domain-name` global configuration command. If there is a period (.) in the hostname, the Cisco IOS software looks up the IP address without appending any default domain name to the hostname.

Follow these steps to set up your switch to use the DNS:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip domain-name name
4. ip name-server server-address1 [server-address2 ... server-address6]
5. ip domain-lookup [nsap | source-interface interface]
6. end
7. show running-config
8. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip domain-name name</td>
<td>Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).</td>
</tr>
<tr>
<td>Example: Switch(config)# ip domain-name Cisco.com</td>
<td>Do not include the initial period that separates an unqualified name from the domain name.</td>
</tr>
<tr>
<td></td>
<td>At boot time, no domain name is configured; however, if the switch configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).</td>
</tr>
<tr>
<td>Step 4 ip name-server server-address1 [server-address2 ... server-address6]</td>
<td>Specifies the address of one or more name servers to use for name and address resolution.</td>
</tr>
</tbody>
</table>
### Command or Action

**Example:**

Switch(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300

<table>
<thead>
<tr>
<th>Step 5</th>
<th>ip domain-lookup [nsap</th>
<th>source-interface interface] Example: Switch(config)# ip domain-lookup</th>
</tr>
</thead>
</table>

You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.

(Optional) Enables DNS-based hostname-to-address translation on your switch. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).

Returns to privileged EXEC mode.

Verifies your entries.

(Optional) Saves your entries in the configuration file.

### Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs in to the switch.

Follow these steps to configure a MOTD login banner:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. banner motd c message c
4. end
5. show running-config
6. copy running-config startup-config

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> banner motd c message c</td>
<td>Specifies the message of the day.</td>
</tr>
<tr>
<td>Example:</td>
<td>c—Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.</td>
</tr>
<tr>
<td>Switch(config)# banner motd #</td>
<td>message—Enters a banner message up to 255 characters. You cannot use the delimiting character in the message.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring a Login Banner

You can configure a login banner to be displayed on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Follow these steps to configure a login banner:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> banner motd c message c</td>
<td>Specifies the message of the day.</td>
</tr>
<tr>
<td>Example:</td>
<td>c—Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.</td>
</tr>
<tr>
<td>Switch(config)# banner motd #</td>
<td>message—Enters a banner message up to 255 characters. You cannot use the delimiting character in the message.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
### SUMMARY STEPS

1. enable
2. configure terminal
3. banner login \textit{c} message \textit{c}
4. end
5. show running-config
6. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  \texttt{Switch> enable}  
  • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  \texttt{Switch# configure terminal} |
| **Step 3** banner login \textit{c} message \textit{c} | Specifies the login message.  
  \textit{c}—Enters the delimiting character of your choice, for example, a pound sign (#), and press the \textbf{Return} key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.  
  \textit{message}—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.  
  Example:  
  \texttt{Switch(config)# banner login \$}  
  Access for authorized users only. Please enter your username and password.  
  \$ |
| **Step 4** end | Returns to privileged EXEC mode.  
  Example:  
  \texttt{Switch(config)# end} |
| **Step 5** show running-config | Verifies your entries.  
  Example:  
  \texttt{Switch# show running-config} |
| **Step 6** copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
  Example:  
  \texttt{Switch(config)# copy running-config startup-config} |
Managing the MAC Address Table

Changing the Address Aging Time

Follow these steps to configure the dynamic address table aging time:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. mac address-table aging-time \([0 \mid 10-1000000]\) \([\text{routed-mac} \mid \text{vlan} \ 	ext{vlan-id}]\)
4. end
5. show running-config
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> mac address-table aging-time ([0 \mid 10-1000000]) ([\text{routed-mac} \mid \text{vlan} \ 	ext{vlan-id}])</td>
<td>Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# mac address-table aging-time 500 vlan 2</td>
<td>The range is 10 to 1000000 seconds. The default is 300. You can also enter 0, which disables aging. Static address entries are never aged or removed from the table.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring MAC Address Change Notification Traps

Follow these steps to configure the switch to send MAC address change notification traps to an NMS host:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. snmp-server host host-addr community-string notification-type { informs | traps } { version { 1 | 2c | 3 } } { vrf vrf instance name }
4. snmp-server enable traps mac-notification change
5. mac address-table notification change
6. mac address-table notification change [ interval value ] [ history-size value ]
7. interface interface-id
8. snmp trap mac-notification change { added | removed }
9. end
10. show running-config
11. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| Step 2 configure terminal | Enters global configuration mode. |
| Example: Switch# configure terminal | |
### Purpose

Specifies the recipient of the trap message.

- **host-addr**—Specifies the name or address of the NMS.
- **traps** (the default)—Sends SNMP traps to the host.
- **informs**—Sends SNMP informs to the host.
- **version**—Specifies the SNMP version to support. Version 1, the default, is not available with informs.
- **community-string**—Specifies the string to send with the notification operation. Though you can set this string by using the `snmp-server host` command, we recommend that you define this string by using the `snmp-server community` command before using the `snmp-server host` command.
- **notification-type**—Uses the `mac-notification` keyword.
- **vrf instance name**—Specifies the VPN routing/forwarding instance for this host.

### Step 3

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`snmp-server host host-addr community-string notification-type { informs</td>
<td>traps } {version {1</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
```

### Step 4

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server enable traps mac-notification change</code></td>
<td>Enables the switch to send MAC address change notification traps to the NMS.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Switch(config)# snmp-server enable traps mac-notification change
```

### Step 5

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac address-table notification change</code></td>
<td>Enables the MAC address change notification feature.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Switch(config)# mac address-table notification change
```

### Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac address-table notification change [interval value] [history-size value]</code></td>
<td>Enters the trap interval time and the history table size.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
```

- (Optional) **interval value**—Specifies the notification trap interval in seconds between each set of traps that are generated to the NMS. The range is 0 to 2147483647 seconds; the default is 1 second.

- (Optional) **history-size value**—Specifies the maximum number of entries in the MAC notification history table. The range is 0 to 500; the default is 1.
### Configuring MAC Address Move Notification Traps

When you configure MAC-move notification, an SNMP notification is generated and sent to the network management system whenever a MAC address moves from one port to another within the same VLAN.

Follow these steps to configure the switch to send MAC address-move notification traps to an NMS host:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `snmp-server host host-addr {traps | informs} {version {1 | 2c | 3}} community-string notification-type`
4. `snmp-server enable traps mac-notification move`
5. `mac address-table notification mac-move`
6. `end`
7. `show running-config`

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td>Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>&lt;br&gt;<strong>Example:</strong> &lt;br&gt;<code>Switch(config)# interface gigabitethernet 0/2</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Enables the MAC address change notification trap on the interface.</td>
</tr>
<tr>
<td>`snmp trap mac-notification change {added</td>
<td>removed}`</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>&lt;br&gt;<strong>Example:</strong> &lt;br&gt;<code>Switch(config)# end</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>&lt;br&gt;<strong>Example:</strong> &lt;br&gt;<code>Switch# show running-config</code></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>&lt;br&gt;<strong>Example:</strong> &lt;br&gt;<code>Switch# copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
8. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`snmp-server host host-addr {traps</td>
<td>informs} {version {1</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>• <code>host-addr</code>—Specifies the name or address of the NMS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>traps</code> (the default)—Sends SNMP traps to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>informs</code>—Sends SNMP informs to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>version</code>—Specifies the SNMP version to support. Version 1, the default, is not available with informs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>community-string</code>—Specifies the string to send with the notification operation. Though you can set this string by using the <code>snmp-server host</code> command, we recommend that you define this string by using the <code>snmp-server community</code> command before using the <code>snmp-server host</code> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>notification-type</code>—Uses the <code>mac-notification</code> keyword.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>snmp-server enable traps mac-notification move</code></td>
<td>Enables the switch to send MAC address move notification traps to the NMS.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>snmp-server enable traps mac-notification move</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>mac address-table notification mac-move</code></td>
<td>Enables the MAC address move notification feature.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>mac address-table notification mac-move</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring MAC Threshold Notification Traps

When you configure MAC threshold notification, an SNMP notification is generated and sent to the network management system when a MAC address table threshold limit is reached or exceeded.

Follow these steps to configure the switch to send MAC address table threshold notification traps to an NMS host:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. snmp-server host host-addr {traps | informs} {version {1 | 2c | 3}} community-string notification-type
4. snmp-server enable traps mac-notification threshold
5. mac address-table notification threshold
6. mac address-table notification threshold threshold [limit percentage] | [interval time]
7. end
8. show running-config
9. copy running-config startup-config

---

### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><em>end</em>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config)# end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show running-config&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch# show running-config</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

---

**What to do next**

To disable MAC address-move notification traps, use the `no snmp-server enable traps mac-notification move` global configuration command. To disable the MAC address-move notification feature, use the `no mac address-table notification mac-move` global configuration command.

You can verify your settings by entering the `show mac address-table notification mac-move` privileged EXEC commands.
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  Example:  
  ```bash
  Switch> enable
  ``` |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  ```bash
  Switch# configure terminal
  ``` |
| **Step 3** snmp-server host host-addr {traps | informs} {version 1 | 2c | 3} community-string notification-type | Specifies the recipient of the trap message.  
  Example:  
  ```bash
  Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
  ``` |
| **Step 4** snmp-server enable traps mac-notification threshold | Enables MAC threshold notification traps to the NMS.  
  Example:  
  ```bash
  Switch(config)# snmp-server enable traps mac-notification threshold
  ``` |
| **Step 5** mac address-table notification threshold | Enables the MAC address threshold notification feature.  
  Example:  
  ```bash
  Switch(config)# mac address-table notification threshold
  ``` |
| **Step 6** mac address-table notification threshold [limit percentage] [interval time] | Enters the threshold value for the MAC address threshold usage monitoring.  
  Example:  
  ```bash
  ``` |
Adding and Removing Static Address Entries

Follow these steps to add a static address:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. mac address-table static mac-addr vlan vlan-id interface interface-id
4. end
5. show running-config
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  enable
  Example:
  Switch> enable | Enables privileged EXEC mode.
  • Enter your password if prompted. |
Purpose

Command or Action | Purpose
--- | ---
Step 2 configure terminal | Enters global configuration mode.
Example: Switch# configure terminal

Step 3 mac address-table static mac-addr vlan vlan-id interface interface-id | Adds a static address to the MAC address table.
Example: Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 0/1
- **mac-addr**—Specifies the destination MAC unicast address to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
- **vlan-id**—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
- **interface-id**—Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast addresses, you can enter multiple interface IDs. For static unicast addresses, you can enter only one interface at a time, but you can enter the command multiple times with the same MAC address and VLAN ID.

Step 4 end | Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.
Example: Switch(config)# end

Step 5 show running-config | Verifies your entries.
Example: Switch# show running-config

Step 6 copy running-config startup-config | (Optional) Saves your entries in the configuration file.
Example: Switch# copy running-config startup-config

Configuring Unicast MAC Address Filtering

Follow these steps to configure the Switch to drop a source or destination unicast static address:

**SUMMARY STEPS**

1. **enable**
2. configure terminal  
3. mac address-table static mac-addr vlan vlan-id drop  
4. end  
5. show running-config  
6. copy running-config startup-config

<table>
<thead>
<tr>
<th>DETAILED STEPS</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**     | enable            | Enables privileged EXEC mode.  
                 | Example:          | • Enter your password if prompted. |
|                 | Switch> enable    |         |
| **Step 2**     | configure terminal | Enters global configuration mode.  
                 | Example:          |         |
|                 | Switch# configure terminal |         |
| **Step 3**     | mac address-table static mac-addr vlan vlan-id drop | Enables unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address.  
                 | Example:          | • mac-addr—Specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped.  
                 | Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop | • vlan-id—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. |
| **Step 4**     | end               | Returns to privileged EXEC mode.  
                 | Example:          |         |
|                 | Switch(config)# end |         |
| **Step 5**     | show running-config | Verifies your entries.  
                 | Example:          |         |
|                 | Switch# show running-config |         |
| **Step 6**     | copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
                 | Example:          |         |
|                 | Switch# copy running-config startup-config |         |
## Monitoring and Maintaining Administration of the Switch

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mac address-table dynamic</td>
<td>Removes all dynamic entries.</td>
</tr>
<tr>
<td>clear mac address-table dynamic address</td>
<td>Removes a specific MAC address.</td>
</tr>
<tr>
<td>clear mac address-table dynamic interface</td>
<td>Removes all addresses on the specified physical port or port channel.</td>
</tr>
<tr>
<td>clear mac address-table dynamic vlan</td>
<td>Removes all addresses on a specified VLAN.</td>
</tr>
<tr>
<td>show clock [detail]</td>
<td>Displays the time and date configuration.</td>
</tr>
<tr>
<td>show ip igmp snooping groups</td>
<td>Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table address mac-address</td>
<td>Displays MAC address table information for the specified MAC address.</td>
</tr>
<tr>
<td>show mac address-table aging-time</td>
<td>Displays the aging time in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table count</td>
<td>Displays the number of addresses present in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table dynamic</td>
<td>Displays only dynamic MAC address table entries.</td>
</tr>
<tr>
<td>show mac address-table interface interface-name</td>
<td>Displays the MAC address table information for the specified interface.</td>
</tr>
<tr>
<td>show mac address-table move update</td>
<td>Displays the MAC address table move update information.</td>
</tr>
<tr>
<td>show mac address-table multicast</td>
<td>Displays a list of multicast MAC addresses.</td>
</tr>
<tr>
<td>show mac address-table notification {change</td>
<td>mac-move</td>
</tr>
<tr>
<td>show mac address-table secure</td>
<td>Displays the secure MAC addresses.</td>
</tr>
<tr>
<td>show mac address-table static</td>
<td>Displays only static MAC address table entries.</td>
</tr>
<tr>
<td>show mac address-table vlan vlan-id</td>
<td>Displays the MAC address table information for the specified VLAN.</td>
</tr>
</tbody>
</table>
Configuration Examples for Switch Administration

Example: Setting the System Clock

This example shows how to manually set the system clock:

```
Switch# clock set 13:32:00 23 July 2013
```

Examples: Configuring Summer Time

This example (for daylight savings time) shows how to specify that summer time starts on March 10 at 02:00 and ends on November 3 at 02:00:

```
Switch(config)# clock summer-time PDT recurring PST date
10 March 2013 2:00 3 November 2013 2:00
```

This example shows how to set summer time start and end dates:

```
Switch(config)# clock summer-time PST date
20 March 2013 2:00 20 November 2013 2:00
```

Example: Configuring a MOTD Banner

This example shows how to configure a MOTD banner by using the pound sign (#) symbol as the beginning and ending delimiter:

```
Switch(config)# banner motd#
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
Switch(config)#
```

This example shows the banner that appears from the previous configuration:

```
Unix> telnet 192.0.2.15
Trying 192.0.2.15...
Connected to 192.0.2.15.
Escape character is '^]'.
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
```
Example: Configuring a Login Banner

This example shows how to configure a login banner by using the dollar sign ($) symbol as the beginning and ending delimiter:

```
Switch(config)# banner login $
Access for authorized users only. Please enter your username and password.$

Switch(config)#
```

Example: Configuring MAC Address Change Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable MAC address notification traps to the NMS, enable the MAC address-change notification feature, set the interval time to 123 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on the specified port:

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 123
Switch(config)# mac address-table notification change history-size 100
Switch(config)# interface gigabitethernet2/1
Switch(config-if)# snmp trap mac-notification change added
```

Example: Configuring MAC Threshold Notification Traps

This example shows how to specify 172.20.10.10 as the NMS, enable the MAC address threshold notification feature, set the interval time to 123 seconds, and set the limit to 78 per cent:

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification threshold
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold interval 123
Switch(config)# mac address-table notification threshold limit 78
```

Example: Adding the Static Address to the MAC Address Table

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination address, the packet is forwarded to the specified port:

```
```
Note

You cannot associate the same static MAC address to multiple interfaces. If the command is executed again with a different interface, the static MAC address is overwritten on the new interface.

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/1
```

Example: Configuring Unicast MAC Address Filtering

This example shows how to enable unicast MAC address filtering and how to configure drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

Additional References for Switch Administration

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch administration commands</td>
<td>Catalyst 2960-X Switch System Management Command Reference</td>
</tr>
<tr>
<td>Network management configuration</td>
<td>Catalyst 2960-X Switch Network Management Configuration Guide</td>
</tr>
<tr>
<td>Layer 2 configuration</td>
<td>Catalyst 2960-X Switch Layer 2 Configuration Guide</td>
</tr>
<tr>
<td>VLAN configuration</td>
<td>Catalyst 2960-X Switch VLAN Management Configuration Guide</td>
</tr>
<tr>
<td>Platform-independent command references</td>
<td>Cisco IOS 15.3M&amp;T Command References</td>
</tr>
<tr>
<td>Platform-independent configuration information</td>
<td>Cisco IOS 15.3M&amp;T Configuration Guides</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for Switch Administration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
</tbody>
</table>
Performing Switch Setup Configuration

• Information About Performing Switch Setup Configuration, on page 935
• How to Perform Switch Setup Configuration, on page 945
• Monitoring Switch Setup Configuration, on page 959
• Configuration Examples for Performing Switch Setup, on page 960
• Additional References for Performing Switch Setup, on page 962
• Feature History and Information For Performing Switch Setup Configuration, on page 963

Information About Performing Switch Setup Configuration

Review the sections in this module before performing your initial switch configuration tasks that include IP address assignments and DHCP autoconfiguration.

Boot Process

To start your switch, you need to follow the procedures in the getting started guide or the hardware installation guide for installing and powering on the switch and setting up the initial switch configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth).

The boot loader software performs the normal boot process and includes these activities:

• Locates the bootable (base) package in the bundle or installed package set.

• Performs low-level CPU initialization. It initializes the CPU registers, which control where physical memory is mapped, its quantity, its speed, and so forth.

• Performs power-on self-test (POST) for the CPU subsystem and tests the system DRAM.

• Initializes the file systems on the system board.

• Loads a default operating system software image into memory and boots up the switch.

The boot loader provides access to the flash file systems before the operating system is loaded. Normally, the boot loader is used only to load, decompress, and start the operating system. After the boot loader gives the operating system control of the CPU, the boot loader is not active until the next system reset or power-on.

The boot loader also provides trap-door access into the system if the operating system has problems serious enough that it cannot be used. The trap-door operation provides enough access to the system so that if it is...
necessary, you can format the flash file system, reinstall the operating system software image by using the
Xmodem Protocol, recover from a lost or forgotten password, and finally restart the operating system.

Before you can assign switch information, make sure that you have connected a PC or terminal to the console
port or a PC to the Ethernet management port, and make sure you have configured the PC or terminal-emulation
software baud rate and character format to match that of the switch console port settings:

• Baud rate default is 9600.
• Data bits default is 8.

Note

If the data bits option is set to 8, set the parity option to none.

• Stop bits default is 2 (minor).
• Parity settings default is none.

Switches Information Assignment

You can assign IP information through the switch setup program, through a DHCP server, or manually.

Use the switch setup program if you want to be prompted for specific IP information. With this program, you
can also configure a hostname and an enable secret password.

It gives you the option of assigning a Telnet password (to provide security during remote management) and
configuring your switch as a command or member switch of a cluster or as a standalone switch.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is
configured.

Note

If you are using DHCP, do not respond to any of the questions in the setup program until the switch receives
the dynamically assigned IP address and reads the configuration file.

If you are an experienced user familiar with the switch configuration steps, manually configure the switch.
Otherwise, use the setup program described in the Boot Process section.

Default Switch Information

Table 96: Default Switch Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and subnet mask</td>
<td>No IP address or subnet mask are defined.</td>
</tr>
<tr>
<td>Default gateway</td>
<td>No default gateway is defined.</td>
</tr>
<tr>
<td>Enable secret password</td>
<td>No password is defined.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The factory-assigned default hostname is Switch.</td>
</tr>
</tbody>
</table>
### DHCP-Based Autoconfiguration Overview

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and an operation for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices. The switch can act as both a DHCP client and a DHCP server.

During DHCP-based autoconfiguration, your switch (DHCP client) is automatically configured at startup with IP address information and a configuration file.

With DHCP-based autoconfiguration, no DHCP client-side configuration is needed on your switch. However, you need to configure the DHCP server for various lease options associated with IP addresses.

If you want to use DHCP to relay the configuration file location on the network, you might also need to configure a Trivial File Transfer Protocol (TFTP) server and a Domain Name System (DNS) server.

The DHCP server for your switch can be on the same LAN or on a different LAN than the switch. If the DHCP server is running on a different LAN, you should configure a DHCP relay device between your switch and the DHCP server. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet.

DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

### DHCP Client Request Process

When you boot up your switch, the DHCP client is invoked and requests configuration information from a DHCP server when the configuration file is not present on the switch. If the configuration file is present and the configuration includes the `ip address dhcp` interface configuration command on specific routed interfaces, the DHCP client is invoked and requests the IP address information for those interfaces.

This is the sequence of messages that are exchanged between the DHCP client and the DHCP server.

#### Figure 61: DHCP Client and Server Message Exchange

The client, Switch A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.
In a DHCPREQUEST broadcast message, the client returns a formal request for the offered configuration information to the DHCP server. The formal request is broadcast so that all other DHCP servers that received the DHCDDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server.

If the configuration parameters sent to the client in the DHCPOFFER unicast message are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means that the offered configuration parameters have not been assigned, that an error has occurred during the negotiation of the parameters, or that the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client).

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address is allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch broadcasts, instead of unicasts, TFTP requests to obtain the switch configuration file.

The DHCP hostname option allows a group of switches to obtain hostnames and a standard configuration from the central management DHCP server. A client (switch) includes in its DCHPDISCOVER message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

If a client has a default hostname (the hostname name global configuration command is not configured or the no hostname global configuration command is entered to remove the hostname), the DHCP hostname option is not included in the packet when you enter the ip address dhcp interface configuration command. In this case, if the client receives the DHCP hostname option from the DHCP interaction while acquiring an IP address for an interface, the client accepts the DHCP hostname option and sets the flag to show that the system now has a hostname configured.

### DHCP-based Autoconfiguration and Image Update

You can use the DHCP image upgrade features to configure a DHCP server to download both a new image and a new configuration file to one or more switches in a network. Simultaneous image and configuration upgrade for all switches in the network helps ensure that each new switch added to a network receives the same image and configuration.

There are two types of DHCP image upgrades: DHCP autoconfiguration and DHCP auto-image update.

### Restrictions for DHCP-based Autoconfiguration

- The DHCP-based autoconfiguration with a saved configuration process stops if there is not at least one Layer 3 interface in an up state without an assigned IP address in the network.
- Unless you configure a timeout, the DHCP-based autoconfiguration with a saved configuration feature tries indefinitely to download an IP address.
• The auto-install process stops if a configuration file cannot be downloaded or if the configuration file is corrupted.

• The configuration file that is downloaded from TFTP is merged with the existing configuration in the running configuration but is not saved in the NVRAM unless you enter the **write memory** or **copy running-configuration startup-configuration** privileged EXEC command. If the downloaded configuration is saved to the startup configuration, the feature is not triggered during subsequent system restarts.

### DHCP Autoconfiguration

DHCP autoconfiguration downloads a configuration file to one or more switches in your network from a DHCP server. The downloaded configuration file becomes the running configuration of the switch. It does not overwrite the bootup configuration saved in the flash, until you reload the switch.

### DHCP Auto-Image Update

You can use DHCP auto-image upgrade with DHCP autoconfiguration to download both a configuration and a new image to one or more switches in your network. The switch (or switches) downloading the new configuration and the new image can be blank (or only have a default factory configuration loaded).

If the new configuration is downloaded to a switch that already has a configuration, the downloaded configuration is appended to the configuration file stored on the switch. (Any existing configuration is not overwritten by the downloaded one.)

To enable a DHCP auto-image update on the switch, the TFTP server where the image and configuration files are located must be configured with the correct option 67 (the configuration filename), option 66 (the DHCP server hostname) option 150 (the TFTP server address), and option 125 (description of the Cisco IOS image file) settings.

After you install the switch in your network, the auto-image update feature starts. The downloaded configuration file is saved in the running configuration of the switch, and the new image is downloaded and installed on the switch. When you reboot the switch, the configuration is stored in the saved configuration on the switch.

### DHCP Server Configuration Guidelines

Follow these guidelines if you are configuring a device as a DHCP server:

• You should configure the DHCP server with reserved leases that are bound to each switch by the switch hardware address.

• If you want the switch to receive IP address information, you must configure the DHCP server with these lease options:
  • IP address of the client (required)
  • Subnet mask of the client (required)
  • DNS server IP address (optional)
  • Router IP address (default gateway address to be used by the switch) (required)

• If you want the switch to receive the configuration file from a TFTP server, you must configure the DHCP server with these lease options:
• TFTP server name (required)
• Boot filename (the name of the configuration file that the client needs) (recommended)
• Hostname (optional)

• Depending on the settings of the DHCP server, the switch can receive IP address information, the configuration file, or both.

• If you do not configure the DHCP server with the lease options described previously, it replies to client requests with only those parameters that are configured. If the IP address and the subnet mask are not in the reply, the switch is not configured. If the router IP address or the TFTP server name are not found, the switch might send broadcast, instead of unicast, TFTP requests. Unavailability of other lease options does not affect autoconfiguration.

• The switch can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your switch but are not configured. (These features are not operational.)

**Purpose of the TFTP Server**

Based on the DHCP server configuration, the switch attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch with all the options required for IP connectivity to the TFTP server, and if you configured the DHCP server with a TFTP server name, address, and configuration filename, the switch attempts to download the specified configuration file from the specified TFTP server.

If you did not specify the configuration filename, the TFTP server, or if the configuration file could not be downloaded, the switch attempts to download a configuration file by using various combinations of filenames and TFTP server addresses. The files include the specified configuration filename (if any) and these files: network-config, cisconet.cfg, hostname.config, or hostname.cfg, where hostname is the switch’s current hostname. The TFTP server addresses used include the specified TFTP server address (if any) and the broadcast address (255.255.255.255).

For the switch to successfully download a configuration file, the TFTP server must contain one or more configuration files in its base directory. The files can include these files:

• The configuration file named in the DHCP reply (the actual switch configuration file).
• The network-config or the cisconet.cfg file (known as the default configuration files).
• The router-config or the ciscorrtr.cfg file (These files contain commands common to all switches. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

If you specify the TFTP server name in the DHCP server-lease database, you must also configure the TFTP server name-to-IP-address mapping in the DNS-server database.

If the TFTP server to be used is on a different LAN from the switch, or if it is to be accessed by the switch through the broadcast address (which occurs if the DHCP server response does not contain all the required information described previously), a relay must be configured to forward the TFTP packets to the TFTP server. The preferred solution is to configure the DHCP server with all the required information.
**Purpose of the DNS Server**

The DHCP server uses the DNS server to resolve the TFTP server name to an IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the switch.

You can configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database. The DNS server can be on the same LAN or on a different LAN from the switch. If it is on a different LAN, the switch must be able to access it through a router.

**Configuring Deep Sleep**

Deep Sleep is a power saving feature that puts the switch into hibernation mode. In this mode, the switch draws very little power. All connected devices also stop drawing power from the switch.

You can configure certain triggers that will put the switch into Deep Sleep mode. Similarly, the switch can wake up from Deep Sleep mode upon certain triggers.

**How to Obtain Configuration Files**

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in these ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).
  
  The switch receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server and upon receipt, it completes its boot up process.

- The IP address and the configuration filename is reserved for the switch, but the TFTP server address is not provided in the DHCP reply (one-file read method).
  
  The switch receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch sends a broadcast message to a TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, it completes its boot-up process.

- Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).
  
  The switch receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the network-config or cisconet.cfg default configuration file. (If the network-config file cannot be read, the switch reads the cisconet.cfg file.)

  The default configuration file contains the hostnames-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its hostname. If the hostname is not found in the file, the switch uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the switch uses the default *Switch* as its hostname.

  After obtaining its hostname from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its hostname (*hostname-config* or *hostname.cfg*, depending
on whether network-config or cisconet.cfg was read earlier) from the TFTP server. If the cisconet.cfg file is read, the filename of the host is truncated to eight characters.

If the switch cannot read the network-config, cisconet.cfg, or the hostname file, it reads the router-config file. If the switch cannot read the router-config file, it reads the ciscortr.cfg file.

---

**Note**

The switch broadcasts TFTP server requests if the TFTP server is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

---

**How to Control Environment Variables**

With a normally operating switch, you enter the boot loader mode only through the console connection. Unplug the switch power cord, then reconnect the power cord. Hold down the **MODE** button until you see the boot loader switch prompt.

The switch boot loader software provides support for nonvolatile environment variables, which can be used to control how the boot loader or any other software running on the system, functions. Boot loader environment variables are similar to environment variables that can be set on UNIX or DOS systems.

Environment variables that have values are stored in flash memory outside of the flash file system.

Each line in these files contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not present; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “” ) is a variable with a value. Many environment variables are predefined and have default values.

Environment variables store two kinds of data:

- Data that controls code, which does not read the Cisco IOS configuration file. For example, the name of a boot loader helper file, which extends or patches the functionality of the boot loader can be stored as an environment variable.

- Data that controls code, which is responsible for reading the Cisco IOS configuration file. For example, the name of the Cisco IOS configuration file can be stored as an environment variable.

You can change the settings of the environment variables by accessing the boot loader or by using Cisco IOS commands. Under normal circumstances, it is not necessary to alter the setting of the environment variables.
Common Environment Variables

This table describes the function of the most common environment variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Boot Loader Command</th>
<th>Cisco IOS Global Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT</td>
<td>set BOOT filesystem :/file-url ...</td>
<td>boot system filesystem :/file-url ...</td>
</tr>
<tr>
<td></td>
<td>A semicolon-separated list of executable files to try to load and execute when</td>
<td>Specifies the Cisco IOS image to load during the next boot cycle on which the image is loaded. This command changes the setting of the BOOT environment variable.</td>
</tr>
<tr>
<td></td>
<td>automatically booting. If the BOOT environment variable is not set, the system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>attempts to load and execute the first executable image it can find by using a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>recursive, depth-first search through the flash file system. If the BOOT variable is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set but the specified images cannot be loaded, the system attempts to boot the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>first bootable file that it can find in the flash file system.</td>
<td></td>
</tr>
<tr>
<td>MANUAL_BOOT</td>
<td>set MANUAL_BOOT yes</td>
<td>boot manual</td>
</tr>
<tr>
<td></td>
<td>Decides whether the switch automatically or manually boots.</td>
<td>Enables manually booting the switch during the next boot cycle and changes the setting of the MANUAL_BOOT environment variable.</td>
</tr>
<tr>
<td></td>
<td>Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts</td>
<td>The next time you reboot the system, the switch is in boot loader mode. To boot up the system, use the boot flash: filesystem :/file-url boot loader command, and specify the name of the bootable image.</td>
</tr>
<tr>
<td></td>
<td>to automatically boot up the system. If it is set to anything else, you must</td>
<td></td>
</tr>
<tr>
<td></td>
<td>manually boot up the switch from the boot loader mode.</td>
<td></td>
</tr>
</tbody>
</table>
**Environment Variables for TFTP**

When the switch is connected to a PC through the Ethernet management port, you can download or upload a configuration file to the boot loader by using TFTP. Make sure the environment variables in this table are configured.

**Table 98: Environment Variables for TFTP**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC_ADDR</td>
<td>Specifies the MAC address of the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> We recommend that you do not modify this variable.</td>
</tr>
<tr>
<td></td>
<td>However, if you modify this variable after the boot loader is up or the value is different from the saved value, enter this command before using TFTP.</td>
</tr>
<tr>
<td>IP_ADDR</td>
<td>Specifies the IP address and the subnet mask for the associated IP subnet of the switch.</td>
</tr>
<tr>
<td>DEFAULT_ROUTER</td>
<td>Specifies the IP address and subnet mask of the default gateway.</td>
</tr>
</tbody>
</table>

**Scheduled Reload of the Software Image**

You can schedule a reload of the software image to occur on the switch at a later time (for example, late at night or during the weekend when the switch is used less), or you can synchronize a reload network-wide (for example, to perform a software upgrade on all switches in the network).

**Note** A scheduled reload must take place within approximately 24 days.
You have these reload options:

- Reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 hours. You can specify the reason for the reload in a string up to 255 characters in length.
- Reload of the software to take place at the specified time (using a 24-hour clock). If you specify the month and day, the reload is scheduled to take place at the specified time and date. If you do not specify the month and day, the reload takes place at the specified time on the current day (if the specified time is later than the current time) or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight.

The `reload` command halts the system. If the system is not set to manually boot up, it reboots itself.

If your switch is configured for manual booting, do not reload it from a virtual terminal. This restriction prevents the switch from entering the boot loader mode and then taking it from the remote user’s control.

If you modify your configuration file, the switch prompts you to save the configuration before reloading. During the save operation, the system requests whether you want to proceed with the save if the `CONFIG_FILE` environment variable points to a startup configuration file that no longer exists. If you proceed in this situation, the system enters setup mode upon reload.

To cancel a previously scheduled reload, use the `reload cancel` privileged EXEC command.

### How to Perform Switch Setup Configuration

Using DHCP to download a new image and a new configuration to a switch requires that you configure at least two switches. One switch acts as a DHCP and TFTP server and the second switch (client) is configured to download either a new configuration file or a new configuration file and a new image file.

### Using the Smartphone App

You can use Cisco’s *Digital Building — Installer* smartphone app to configure your switch.

This app allows you to:

- Connect to the switch from your smartphone via Bluetooth.
- View details of the switch, such as MAC Address, software image version, and operating temperature.
- Change the switch’s name and password.
- Turn on or off (make available or unavailable) each downlink port on a switch. This will enable or disable endpoints connected to those ports.
- View the details of each endpoint connected to the ports.
- Update the switch’s firmware image with a new version.
- Install a pre-defined or modified configuration template on the switch.
- Back up the switch’s firmware image to the smartphone.
- Generate a report for the switch and send via email to a recipient.

To install the app, look for the *Digital Building — Installer* app in the Google Play Store or the iOS App Store.
Minimum mobile OS requirements for the app:

- Android 4.4.2 and higher
- iOS 9 and higher

## Configuring DHCP Autoconfiguration (Only Configuration File)

This task describes how to configure DHCP autoconfiguration of the TFTP and DHCP settings on an existing switch in the network so that it can support the autoconfiguration of a new switch.

### SUMMARY STEPS

1. configure terminal
2. ip dhcp pool poolname
3. boot filename
4. network network-number mask prefix-length
5. default-router address
6. option 150 address
7. exit
8. tftp-server flash:filename.text
9. interface interface-id
10. no switchport
11. ip address address mask
12. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ip dhcp pool poolname</td>
<td>Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip dhcp pool pool</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> boot filename</td>
<td>Specifies the name of the configuration file that is used as a boot image.</td>
</tr>
<tr>
<td>Example: Switch(dhcp-config)# boot config-boot.text</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>4</td>
<td><code>network network-number mask prefix-length</code></td>
</tr>
<tr>
<td></td>
<td>Example: Switch (dhcp-config)# <code>network 10.10.0.0 255.255.255.0</code></td>
</tr>
<tr>
<td>5</td>
<td><code>default-router address</code></td>
</tr>
<tr>
<td></td>
<td>Example: Switch (dhcp-config)# <code>default-router 10.10.10.1</code></td>
</tr>
<tr>
<td>6</td>
<td><code>option 150 address</code></td>
</tr>
<tr>
<td></td>
<td>Example: Switch (dhcp-config)# <code>option 150 10.10.10.1</code></td>
</tr>
<tr>
<td>7</td>
<td><code>exit</code></td>
</tr>
<tr>
<td></td>
<td>Example: Switch (dhcp-config)# <code>exit</code></td>
</tr>
<tr>
<td>8</td>
<td><code>tftp-server flash:filename.text</code></td>
</tr>
<tr>
<td></td>
<td>Example: Switch (config)# <code>tftp-server flash:config-boot.text</code></td>
</tr>
<tr>
<td>9</td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td></td>
<td>Example: Switch (config)# <code>interface gigabitethernet 0/4</code></td>
</tr>
<tr>
<td>10</td>
<td><code>no switchport</code></td>
</tr>
<tr>
<td></td>
<td>Example: Switch (config-if)# <code>no switchport</code></td>
</tr>
<tr>
<td>11</td>
<td><code>ip address address mask</code></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# ip address 10.10.10.1 255.255.255.0</td>
<td></td>
</tr>
</tbody>
</table>

### Step 12

End

**Example:**

Switch(config-if)# end

Returns to privileged EXEC mode.

---

**Related Topics**

Example: Configuring a Switch as a DHCP Server, on page 960

### Configuring DHCP Auto-Image Update (Configuration File and Image)

This task describes DHCP autoconfiguration to configure TFTP and DHCP settings on an existing switch to support the installation of a new switch.

**Before you begin**

You must first create a text file (for example, autoinstall dhcp) that will be uploaded to the switch. In the text file, put the name of the image that you want to download (for example, c3750e-ipservices-mz.122-44.3.SE.tarc3750x-ipservices-mz.122-53.3.SE2.tar). This image must be a tar and not a bin file.

**SUMMARY STEPS**

1. configure terminal
2. ip dhcp pool poolname
3. boot filename
4. network network-number mask prefix-length
5. default-router address
6. option 150 address
7. option 125 hex
8. copy tftp flash filename.txt
9. copy tftp flash imagename.bin
10. exit
11. tftp-server flash: config.text
12. tftp-server flash: imagename.bin
13. tftp-server flash: filename.txt
14. interface interface-id
15. no switchport
16. ip address address mask
17. end
18. copy running-config startup-config
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Example: Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip dhcp pool <em>poolname</em>&lt;br&gt;Example: Switch(config)# ip dhcp pool pool1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>boot filename</code>&lt;br&gt;Example: Switch(dhcp-config)# boot config-boot.text</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>network network-number mask prefix-length</code>&lt;br&gt;Example: Switch(dhcp-config)# network 10.10.0.0 255.255.255.0</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>default-router address</code>&lt;br&gt;Example: Switch(dhcp-config)# default-router 10.10.1</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>option 150 address</code>&lt;br&gt;Example: Switch(dhcp-config)# option 150 10.10.1</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>option 125 hex</code>&lt;br&gt;Example: Switch(dhcp-config)# option 125 hex</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Purpose</strong></td>
</tr>
</tbody>
</table>
| copy tftp flash filename.txt | Uploads the text file to the switch.  
Example:  
Switch(config)# copy tftp flash image.bin |
| **Step 9** | **Purpose** |
| copy tftp flash imagename.bin | Uploads the tar file for the new image to the switch.  
Example:  
Switch(config)# copy tftp flash image.bin |
| **Step 10** | **Purpose** |
| exit | Returns to global configuration mode.  
Example:  
Switch(dhcp-config)# exit |
| **Step 11** | **Purpose** |
| tftp-server flash: config.text | Specifies the Cisco IOS configuration file on the TFTP server.  
Example:  
Switch(config)# tftp-server flash:config-boot.text |
| **Step 12** | **Purpose** |
| tftp-server flash: imagename.bin | Specifies the image name on the TFTP server.  
Example:  
Switch(config)# tftp-server flash:image.bin |
| **Step 13** | **Purpose** |
| tftp-server flash: filename.txt | Specifies the text file that contains the name of the image file to download  
Example:  
Switch(config)# tftp-server flash:boot-config.text |
| **Step 14** | **Purpose** |
| interface interface-id | Specifies the address of the client that will receive the configuration file.  
Example:  
Switch(config)# interface gigabitethernet 0/4 |
| **Step 15** | **Purpose** |
| no switchport | Puts the interface into Layer 3 mode.  
Example:  
Switch(config-if)# no switchport |
### Purpose

**Command or Action**

**Step 16**  
`ip address address mask`  
Example:  
`Switch(config-if)# ip address 10.10.10.1 255.255.255.0`

**Step 17**  
`end`  
Example:  
`Switch(config-if)# end`

**Step 18**  
`copy running-config startup-config`  
Example:  
`Switch(config-if)# end`

### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address and mask for the interface.</td>
<td><code>ip address address mask</code></td>
</tr>
<tr>
<td>Returns to privileged EXEC mode.</td>
<td><code>end</code></td>
</tr>
<tr>
<td>(Optional) Saves your entries in the configuration file.</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

### Related Topics

Example: Configuring DHCP Auto-Image Update, on page 961

## Configuring the Client to Download Files from DHCP Server

### Note

You should only configure and enable the Layer 3 interface. Do not assign an IP address or DHCP-based autoconfiguration with a saved configuration.

### SUMMARY STEPS

1. configure terminal  
2. boot host dhcp  
3. boot host retry timeout `timeout-value`  
4. banner config-save `^C warning-message ^C`  
5. `end`  
6. show boot

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Step 2 | `boot host dhcp`  
Example:  
`Switch(conf)# boot host dhcp` | Enables autoconfiguration with a saved configuration. |
|--------|--------------------------------------------------|
| Step 3 | `boot host retry timeout timeout-value`  
Example:  
`Switch(conf)# boot host retry timeout 300` | (Optional) Sets the amount of time the system tries to download a configuration file.  
**Note** If you do not set a timeout, the system will try indefinitely to obtain an IP address from the DHCP server. |
| Step 4 | `banner config-save ^C warning-message ^C`  
Example:  
`Switch(conf)# banner config-save ^C Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C` | (Optional) Creates warning messages to be displayed when you try to save the configuration file to NVRAM. |
| Step 5 | `end`  
Example:  
`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| Step 6 | `show boot`  
Example:  
`Switch# show boot` | Verifies the configuration. |

### Related Topics

- Example: Configuring a Switch to Download Configurations from a DHCP Server, on page 961

### Routing Assistance When IP Routing is Disabled

These mechanisms allow the Switch to learn about routes to other networks when it does not have IP routing enabled:

- Default Gateway

### Default Gateway

Another method for locating routes is to define a default router or default gateway. All non-local packets are sent to this router, which either routes them appropriately or sends an IP Control Message Protocol (ICMP) redirect message back, defining which local router the host should use. The Switch caches the redirect messages.
and forwards each packet as efficiently as possible. A limitation of this method is that there is no means of
detecting when the default router has gone down or is unavailable.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip default-gateway ip-address</td>
<td>Sets up a default gateway (router).</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip default gateway 10.1.5.1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip redirects</td>
<td>Displays the address of the default gateway router to verify the setting.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show ip redirects</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring the NVRAM Buffer Size**

The default NVRAM buffer size is 512 KB. In some cases, the configuration file might be too large to save to NVRAM. You can configure the size of the NVRAM buffer to support larger configuration files.

**Note**

After you configure the NVRAM buffer size, reload the switch.
SUMMARY STEPS

1. configure terminal
2. boot buffersize size
3. end
4. show boot

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> boot buffersize size</td>
<td>Configures the NVRAM buffersize in KB. The valid range for size is from 4096 to 1048576.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# boot buffersize 524288</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show boot</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show boot</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

Example: Configuring NVRAM Buffer Size, on page 962

Configuring the Switch to Enter Deep Sleep Mode

You can configure several triggers that will put the switch into Deep Sleep mode.

Triggers that put the switch to sleep are:

- Using EnergyWise to hibernate the switch at a specified time
- A COAP CLI command
- A COAP command over HTTP that sends a payload data packet to the switch
Using EnergyWise

You can use an EnergyWise Level 1 command to put the switch into hibernation mode automatically at a specified time. This will use the real-time clock that runs on the switch. This hibernation mode will cause the switch to enter Deep Sleep mode.

For details on using the EnergyWise Level 1 command, see the Configuring Hibernation Start and End Times section in the Configuring EnergyWise chapter of this book.

CLI COAP Command

You can use a COAP command to put the switch into Deep Sleep mode immediately.

In the global configuration mode, enter the command `coap sleep wol [enable | disable]`. This will put the switch into Deep Sleep mode immediately.

- `enable` - The switch will listen for incoming packets in the uplink ports in order to wake up.
- `disable` - The switch cannot be woken up from packets sent to the uplink ports. In this case, the only way to wake up the switch is to press the MODE button.

Send Payload Data

You can configure the switch to enter Deep Sleep mode when a packet of data (payload) is sent to the switch. This packet is sent via COAP over HTTP.

To send payload data:

1. Use a REST client and connect to the switch by going to the URL `http://<Switch IP>/level/15/coap/cisco/sleep`.
2. POST with payload `"data={"WOL":1}"`.

Enter “WOL” : 1 if you want the switch to listen for incoming packets in the uplink ports in order to wake up. Enter “WOL” : 0 if you do not want the switch to listen for incoming packets in the uplink ports in order to wake up. In this case, the only way to wake up the switch is to press the MODE button.

Configuring the Switch to Wake Up From Deep Sleep Mode

You can configure several triggers that will wake up the switch from Deep Sleep mode.

Triggers that wake up the switch from Deep Sleep mode are:

- Using EnergyWise to wake up the switch at a specified time
- A COAP command that sends a payload data packet to the switch
- Pressing the MODE button on the switch

Using EnergyWise

If you have configured an EnergyWise Level 1 command to put the switch into Deep Sleep mode at a specified time, the same configuration is used to wake up the switch at a specified time. This will use the real-time clock that runs on the switch.
Send Payload Data
You can configure the switch to wake up from Deep Sleep mode when a packet of data (payload) is sent to the switch. This packet is sent via COAP.

To send payload data:
1. Use a REST client and connect to the switch by going to the URL `coap://<switch IP>/cisco/sleep`.
2. POST with payload `{"level":"10"}`.

MODE Button
Press and hold the **MODE** button on the switch for 5 seconds to wake up the switch from Deep Sleep mode.

Modifying the Switch Startup Configuration

Specifying the Filename to Read and Write the System Configuration
By default, the Cisco IOS software uses the `config.text` file to read and write a nonvolatile copy of the system configuration. However, you can specify a different filename, which will be loaded during the next boot cycle.

Before you begin
Use a standalone switch for this task.

SUMMARY STEPS
1. `configure terminal`
2. `boot flash:/file-url`
3. `end`
4. `show boot`
5. `copy running-config startup-config`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 2</strong></th>
<th>Specifies the configuration file to load during the next boot cycle.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>boot flash:/file-url</code></td>
<td><code>file-url</code>—The path (directory) and the configuration filename. Filenames and directory names are case-sensitive.</td>
</tr>
<tr>
<td>Example: Switch(config)# boot flash:config.text</td>
<td></td>
</tr>
</tbody>
</table>
Manually Booting the Switch

By default, the switch automatically boots up; however, you can configure it to manually boot up.

Before you begin

Use a standalone switch for this task.

SUMMARY STEPS

1. configure terminal
2. boot manual
3. end
4. show boot
5. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>boot manual</td>
<td>Enables the switch to manually boot up during the next boot cycle.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# boot manual</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Scheduled Software Image Reload

This task describes how to configure your switch to reload the software image at a later time.

**SUMMARY STEPS**

1. configure terminal
2. copy running-config startup-config
3. reload in [hh:mm [text]
4. reload at hh:mm [month day | day month] [text]
5. reload cancel
6. show reload

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

---

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> show boot</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch#</td>
<td></td>
</tr>
</tbody>
</table>

The `boot manual` global command changes the setting of the MANUAL_BOOT environment variable.

The next time you reboot the system, the switch is in boot loader mode, shown by the `switch:` prompt. To boot up the system, use the `boot filesystem:/file-url` boot loader command.

- `filesystem:`—Uses flash: for the system board flash device.
  - `switch: boot flash`:
- `file-url`—Specifies the path (directory) and the name of the bootable image.

Filenames and directory names are case-sensitive.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch#</td>
<td></td>
</tr>
</tbody>
</table>

---

---

**Configuring a Scheduled Software Image Reload**

This task describes how to configure your switch to reload the software image at a later time.

**SUMMARY STEPS**

1. configure terminal
2. copy running-config startup-config
3. reload in [hh:mm [text]
4. reload at hh:mm [month day | day month] [text]
5. reload cancel
6. show reload

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)#</td>
<td></td>
</tr>
</tbody>
</table>

The `boot manual` global command changes the setting of the MANUAL_BOOT environment variable.

The next time you reboot the system, the switch is in boot loader mode, shown by the `switch:` prompt. To boot up the system, use the `boot filesystem:/file-url` boot loader command.

- `filesystem:`—Uses flash: for the system board flash device.
  - `switch: boot flash`:
- `file-url`—Specifies the path (directory) and the name of the bootable image.

Filenames and directory names are case-sensitive.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> show boot</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch#</td>
<td></td>
</tr>
</tbody>
</table>

The `boot manual` global command changes the setting of the MANUAL_BOOT environment variable.

The next time you reboot the system, the switch is in boot loader mode, shown by the `switch:` prompt. To boot up the system, use the `boot filesystem:/file-url` boot loader command.

- `filesystem:`—Uses flash: for the system board flash device.
  - `switch: boot flash`:
- `file-url`—Specifies the path (directory) and the name of the bootable image.

Filenames and directory names are case-sensitive.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch#</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Saves your switch configuration information to the startup configuration before you use the <strong>reload</strong> command.</td>
</tr>
</tbody>
</table>

**Step 2**

**copy running-config startup-config**

**Example:**

```
copy running-config startup-config
```

Saves your switch configuration information to the startup configuration before you use the **reload** command.

**Step 3**

**reload in \[hh\:\]mm \[text\]**

**Example:**

```
Switch(config)# reload in 12
```

```
System configuration has been modified. Save? [yes/no]: y
```

Schedules a reload of the software to take affect in the specified minutes or hours and minutes. The reload must take place within approximately 24 days. You can specify the reason for the reload in a string up to 255 characters in length.

**Step 4**

**reload at hh: mm \[month day | day month\] \[text\]**

**Example:**

```
Switch(config)# reload at 14:00
```

Specifies the time in hours and minutes for the reload to occur.

**Note**  Use the **at** keyword only if the switch system clock has been set (through Network Time Protocol (NTP), the hardware calendar, or manually). The time is relative to the configured time zone on the switch. To schedule reloads across several switches to occur simultaneously, the time on each switch must be synchronized with NTP.

**Step 5**

**reload cancel**

**Example:**

```
Switch(config)# reload cancel
```

Cancels a previously scheduled reload.

**Step 6**

**show reload**

**Example:**

```
show reload
```

Displays information about a previously scheduled reload or identifies if a reload has been scheduled on the switch.

---

**Monitoring Switch Setup Configuration**

**Example: Verifying the Switch Running Configuration**

```
Switch# show running-config
Building configuration...

Current configuration: 1363 bytes
```

---

**Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)**
Examples: Displaying Software Install

This example displays software bootup in install mode:

```
switch# boot flash:/c2960x-universalk9-mz-150-2.EX/c2960x-universalk9-mz-150-2.EX.bin
```

Configuration Examples for Performing Switch Setup

**Example: Configuring a Switch as a DHCP Server**

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# boot config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# interface gigabitethernet 0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
```
Example: Configuring DHCP Auto-Image Update

Switch(config-if)# end

Related Topics
Configuring DHCP Autoconfiguration (Only Configuration File), on page 946

Example: Configuring DHCP Auto-Image Update

Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# boot config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e74.73.7461.6c6c.5f686370
Switch(config)# exit
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:image_name
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitethernet 0/4
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end

Related Topics
Configuring DHCP Auto-Image Update (Configuration File and Image), on page 948

Example: Configuring a Switch to Download Configurations from a DHCP Server

This example uses a Layer 3 SVI interface on VLAN 99 to enable DHCP-based autoconfiguration with a saved configuration:

Switch# configure terminal
Switch(config)# boot host dhcp
Switch(config)# boot host retry timeout 300
Switch(config)# banner config-save 
"Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot"
Switch(config)# vlan 99
Switch(config-vlan)# interface vlan 99
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch# show boot
BOOT path-list:
Config file: flash://config.text
Private Config file: flash://private-config.text
Enable Break: no
Manual Boot: no
HELPER path-list:
NVRAM/Config file buffer size: 32768
Timeout for Config Download: 300 seconds
Example: Configuring NVRAM Buffer Size

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# boot buffersize 600000
Switch(config)# end
Switch# show boot
BOOT path-list :
Config file : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break : no
Manual Boot : no
HELPER path-list :
Auto upgrade : yes
Auto upgrade path :
NVRAM/Config file
 buffer size: 600000
Timeout for Config Download: 300 seconds
Config Download
 via DHCP: enabled (next boot: enabled)
Switch#
```

Related Topics
Configuring the NVRAM Buffer Size, on page 953

Additional References for Performing Switch Setup

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch setup commands</td>
<td>Catalyst 2960-X Switch System Management Command Reference</td>
</tr>
<tr>
<td>Boot loader commands</td>
<td></td>
</tr>
<tr>
<td>USB flash devices</td>
<td>Catalyst 2960-X Switch Interface and Hardware Component Configuration Guide</td>
</tr>
<tr>
<td>Hardware installation</td>
<td>Catalyst 2960-X Switch Managing Cisco IOS Image Files Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Catalyst 2960-X Switch Hardware Installation Guide</td>
</tr>
</tbody>
</table>
 Cisco IOS 15.3M&T Command References

Platform-independent command references
Cisco IOS 15.3M&T Command References

Platform-independent configuration information
Cisco IOS 15.3M&T Configuration Guides

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For Performing Switch Setup Configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
Restrictions for Configuring System Message Logs

When the `logging discriminator` command is configured, the device may experience memory leak or crash. This usually happens during heavy syslog or debug output. The rate of the memory leak is dependent on the number of logs being produced. In extreme cases, the device may also crash. As a workaround, use the `no logging discriminator` command to disable the logging discriminator.

Information About Configuring System Message Logs

System Message Logging

By default, a switch sends the output from system messages and `debug` privileged EXEC commands to a logging process. Stack members can trigger system messages. A stack member that generates a system message appends its hostname in the form of hostname-n, where n is a switch range from 1 to 8, and redirects the output to the logging process on the active switch. Though the active switch is a stack member, it does not append its hostname to system messages. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the active consoles after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time
debugging and management. For information on possible messages, see the system message guide for this
release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them
to a properly configured syslog server. The switch software saves syslog messages in an internal buffer on a
standalone switch, and in the case of a switch stack, on the active switch. If a standalone switch or the stack
master fails, the log is lost unless you had saved it to flash memory.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch
through Telnet, through the console port, or through the Ethernet management port. In a switch stack, all stack
member consoles provide the same console output.

Note
The syslog format is compatible with 4.3 BSD UNIX.

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional
sequence number or time-stamp information, if configured. Depending on the switch, messages appear in one
of these formats:

- seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)
- seq no:timestamp: %facility-severity-MNEMONIC:description

The part of the message preceding the percent sign depends on the setting of these global configuration
commands:

- service sequence-numbers
- service timestamps log datetime
- service timestamps log datetime [localtime] [msec] [show-timezone]
- service timestamps log uptime

Table 99: System Log Message Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq no:</td>
<td>Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured.</td>
</tr>
<tr>
<td>timestamp formats:</td>
<td>Date and time of the message or event. This information appears only if the service timestamps log [datetime</td>
</tr>
<tr>
<td>mm/dd h h:mm:ss</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>hh:mm:ss (short uptime)</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>d h (long uptime)</td>
<td></td>
</tr>
</tbody>
</table>
### Default System Message Logging Settings

**Table 100: Default System Message Logging Settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>System message logging to the console</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Console severity</td>
<td>Debugging.</td>
</tr>
<tr>
<td>Logging file configuration</td>
<td>No filename specified.</td>
</tr>
<tr>
<td>Logging buffer size</td>
<td>4096 bytes.</td>
</tr>
<tr>
<td>Logging history size</td>
<td>1 message.</td>
</tr>
<tr>
<td>Time stamps</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Synchronous logging</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Logging server</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Syslog server IP address</td>
<td>None configured.</td>
</tr>
<tr>
<td>Server facility</td>
<td>Local7</td>
</tr>
<tr>
<td>Server severity</td>
<td>Informational.</td>
</tr>
</tbody>
</table>

### Enabling Syslog Trap Messages

You can enable Syslog traps using the `snmp-server enable traps syslog` command.

After enabling Syslog traps, you have to specify the trap message severity. Use the `logging snmp-trap` command to specify the trap level. By default, the command enables severity 0 to 4. To enable all the severity level, configure the `logging snmp-trap 0 7` command.

To enable individual trap levels, configure the following commands:

- `logging snmp-trap emergencies`: Enables only severity 0 traps.
- **logging snmp-trap alert** Enables only severity 1 traps.

Note that, along with the Syslog traps, the Syslog history should also be applied. Without this configuration, Syslog traps are not sent.

Use the **logging history informational** command to enable the Syslog history.

## How to Configure System Message Logs

### Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. This task is optional.

#### SUMMARY STEPS

1. `configure terminal`
2. `logging buffered [size]`
3. `logging host`
4. `logging file flash: filename [max-file-size [min-file-size]] [severity-level-number | type]`
5. `end`
6. `terminal monitor`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> logging buffered [size]</td>
<td>Logs messages to an internal buffer on the switch. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# logging buffered 8192</td>
<td>If a standalone switch or the active switch fails, the log file is lost unless you previously saved it to flash memory. See Step 4.</td>
</tr>
</tbody>
</table>

**Note** Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should **not** be set to this amount.
### Command or Action

| Step 3 | logging host  
Example:  
Switch(config)# logging 125.1.1.100 | Logs messages to a UNIX syslog server host.  
*host* specifies the name or IP address of the host to be used as the syslog server.  
To build a list of syslog servers that receive logging messages, enter this command more than once. |

| Step 4 | logging file flash: filename [max-file-size [min-file-size]] [severity-level-number | type]  
Example:  
Switch(config)# logging file flash:log_msg.txt 40960 4096 3 | Stores log messages in a file in flash memory on a standalone switch.  
- *filename*—Enters the log message filename.  
- (Optional) **max-file-size**—Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes.  
- (Optional) **min-file-size**—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes.  
- (Optional) **severity-level-number | type**—Specifies either the logging severity level or the logging type. The severity range is 0 to 7. |

| Step 5 | end  
Example:  
Switch(config)# end | Returns to privileged EXEC mode. |

| Step 6 | terminal monitor  
Example:  
Switch# terminal monitor | Logs messages to a nonconsole terminal during the current session.  
Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages. |

### Synchronizing Log Messages

You can synchronize unsolicited messages and **debug** privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or is printed. Unsolicited messages and **debug** command output appears on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.
This task is optional.

**SUMMARY STEPS**

1. `configure terminal`  
2. `line [console | vty] line-number [ending-line-number]`  
3. `logging synchronous [level {severity-level | all} | limit number-of-buffers]`  
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** configure terminal  
  Example:
  Switch# configure terminal | Enters global configuration mode. |
| **Step 2** line [console | vty] line-number [ending-line-number]  
  Example:
  Switch(config)# line console | Specifies the line to be configured for synchronous logging of messages.  
  - `console` — Specifies configurations that occur through the switch console port or the Ethernet management port.  
  - `line vty line-number` — Specifies which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15.  
  You can change the setting of all 16 vty lines at once by entering:  
  `line vty 0 15`  
  You can also change the setting of the single vty line being used for your current connection. For example, to change the setting for vty line 2, enter:  
  `line vty 2`  
  When you enter this command, the mode changes to line configuration. |
| **Step 3** `logging synchronous [level {severity-level | all} | limit number-of-buffers]`  
  Example:  
  Switch(config)# logging synchronous level 3 limit 1000 | Enables synchronous logging of messages.  
  - (Optional) `level severity-level` — Specifies the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2. |
### Disabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press `Return`.

To reenable message logging after it has been disabled, use the **logging on** global configuration command. This task is optional.

### SUMMARY STEPS

1. `configure terminal`
2. `no logging console`
3. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  - `configure terminal`
  - Example:
  - `Switch(config)# configure terminal`
| Enters global configuration mode. |
| **Step 2**
  - `no logging console`
  - Example: |
  - Disables message logging. |
### Purpose

Command or Action  | Purpose
--- | ---

| Switch(config)# no logging console |

### Step 3

**Example:**

| Switch(config)# end |

---

### Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time-stamped.

This task is optional.

#### SUMMARY STEPS

1. `configure terminal`
2. Use one of these commands:
   - `service timestamps log uptime`
   - `service timestamps log datetime[msec | localtime | show-timezone]`
3. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `configure terminal`  
**Example:**  
`Switch# configure terminal` |

Enters global configuration mode.

| **Step 2**  
**Example:**  
`Switch(config)# service timestamps log uptime`  
or  
`Switch(config)# service timestamps log datetime` |

Uses one of these commands:

- `log uptime`—Enables time stamps on log messages, showing the time since the system was rebooted.
- `log datetime`—Enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.

| **Step 3**  
**Example:** |

Returns to privileged EXEC mode.
Enabling and Disabling Sequence Numbers in Log Messages

If there is more than one log message with the same time stamp, you can display messages with sequence numbers to view these messages. By default, sequence numbers in log messages are not displayed. This task is optional.

**SUMMARY STEPS**

1. configure terminal
2. service sequence-numbers
3. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# end</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 1 configure terminal Example: Switch# configure terminal</td>
<td>Enables sequence numbers.</td>
</tr>
<tr>
<td>Step 2 service sequence-numbers Example: Switch(config)# service sequence-numbers</td>
<td></td>
</tr>
<tr>
<td>Step 3 end Example: Switch(config)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Defining the Message Severity Level

Limit messages displayed to the selected device by specifying the severity level of the message. This task is optional.

**SUMMARY STEPS**

1. configure terminal
2. logging console level
### Limiting Syslog Messages Sent to the History Table and to SNMP

This task explains how to limit syslog messages that are sent to the history table and to SNMP.

This task is optional.

#### SUMMARY STEPS

1. configure terminal
2. logging history level
3. logging history size number
4. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>logging console level</td>
<td>Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# logging console 3</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>logging monitor level</td>
<td>Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# logging monitor 3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>logging trap level</td>
<td>Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# logging trap 3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> logging history level</td>
<td>Changes the default level of syslog messages stored in the history file and sent to the SNMP server. By default, <strong>warnings</strong>, <strong>errors</strong>, <strong>critical</strong>, <strong>alerts</strong>, and <strong>emergencies</strong> messages are sent.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# logging history 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> logging history size number</td>
<td>Specifies the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 0 to 500 messages.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# logging history size 200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Logging Messages to a UNIX Syslog Daemon

This task is optional.

---

**Note**

Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX `man syslogd` command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

---

**Before you begin**

- Log in as root.
- Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server.

**SUMMARY STEPS**

1. Add a line to the file `/etc/syslog.conf`.
2. Enter these commands at the UNIX shell prompt.
3. Make sure the syslog daemon reads the new changes.
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | Add a line to the file `/etc/syslog.conf`.  
**Example:**  
`local7.debug /usr/adm/logs/cisco.log` | • **local7**—Specifies the logging facility.  
• **debug**—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it. |
| **Step 2** | Enter these commands at the UNIX shell prompt.  
**Example:**  
```bash  
$ touch /var/log/cisco.log  
$ chmod 666 /var/log/cisco.log  
``` | Creates the log file. The syslog daemon sends messages at this level or at a more severe level to this file. |
| **Step 3** | Make sure the syslog daemon reads the new changes.  
**Example:**  
```bash  
$ kill -HUP `cat /etc/syslog.pid`  
``` | For more information, see the `man syslog.conf` and `man syslogd` commands on your UNIX system. |

### Monitoring and Maintaining System Message Logs

#### Monitoring Configuration Archive Logs

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show archive log config {all</td>
<td>number [end-number]</td>
</tr>
</tbody>
</table>

### Configuration Examples for System Message Logs

#### Example: Switch System Message

This example shows a partial switch system message on a switch:

- `00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up`
- `00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up`
- `00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up`
- `00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down`
- `00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down`
Examples: Displaying Service Timestamps Log

This example shows part of a logging display with the service timestamps log datetime global configuration command enabled:

```
*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the service timestamps log uptime global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
```

This example shows part of a logging display with the sequence numbers enabled.

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) (Switch-2)
```

Additional References for System Message Logs

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System message log commands</td>
<td>Catalyst 2960-X Switch System Management Command Reference</td>
</tr>
<tr>
<td></td>
<td>Catalyst 2960-L Switch System Management Command Reference</td>
</tr>
<tr>
<td>Platform-independent command references</td>
<td>Cisco IOS 15.3M&amp;T Command References</td>
</tr>
<tr>
<td>Platform-independent configuration information</td>
<td>Cisco IOS 15.3M&amp;T Configuration Guides</td>
</tr>
</tbody>
</table>
Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information For System Message Logs

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
Information About Configuring Online Diagnostics

Online Diagnostics

With online diagnostics, you can test and verify the hardware functionality of the Switch while the Switch is connected to a live network.

The online diagnostics contain packet switching tests that check different hardware components and verify the data path and the control signals.

The online diagnostics detect problems in these areas:

- Hardware components
- Interfaces (Ethernet ports and so forth)
- Solder joints

Online diagnostics are categorized as on-demand, scheduled, or health-monitoring diagnostics. On-demand diagnostics run from the CLI; scheduled diagnostics run at user-designated intervals or at specified times when the Switch is connected to a live network; and health-monitoring runs in the background with user-defined intervals. By default, the health-monitoring test runs for every 30 seconds.

After you configure online diagnostics, you can manually start diagnostic tests or display the test results. You can also see which tests are configured for the Switch and the diagnostic tests that have already run.

Note

The Catalyst 2960L switch is not stackable. Hence, the switch number keyword is not supported on this switch.
How to Configure Online Diagnostics

Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the switch, use the `diagnostic start` privileged EXEC command to begin diagnostic testing.

After starting the tests, you cannot stop the testing process.

Use this privileged EXEC command to manually start online diagnostic testing.

**SUMMARY STEPS**

1. `diagnostic start test {name | test-id | test-id-range | all | basic | non-disruptive }`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| **diagnostic start test {name | test-id | test-id-range | all | basic | non-disruptive }** |
| **Example:**
| Switch# diagnostic start test basic |

You can specify the tests by using one of these options:

- **name**—Enters the name of the test.
- **test-id**—Enters the ID number of the test.
- **test-id-range**—Enters the range of test IDs by using integers separated by a comma and a hyphen.
- **all**—Starts all of the tests.
- **basic**—Starts the basic test suite.
- **non-disruptive**—Starts the non-disruptive test suite.

Configuring Online Diagnostics

You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

Scheduling Online Diagnostics

You can schedule online diagnostics to run at a designated time of day or on a daily, weekly, or monthly basis for a switch. Use the `no` form of this command to remove the scheduling.

**SUMMARY STEPS**

1. `configure terminal`
2. `diagnostic schedule test {name | test-id | test-id-range | all | basic | non-disruptive |} {daily | on mm dd yyyy hh:mm | weekly day-of-week hh:mm}`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Schedules on-demand diagnostic tests for a specific day and time. |
| diagnostic schedule test {name | test-id | test-id-range | all | basic | non-disruptive | | daily | on mm dd yyyy hh:mm | weekly | day-of-week hh:mm} |  |
| Example: Switch(config)# diagnostic schedule test 1-5 on July 3 2013 23:10 |  |

When specifying the tests to be scheduled, use these options:

- **name**—Name of the test that appears in the `show diagnostic content` command output.
- **test-id**—ID number of the test that appears in the `show diagnostic content` command output.
- **test-id-range**—ID numbers of the tests that appear in the `show diagnostic content` command output.
- **all**—All test IDs.
- **basic**—Starts the basic on-demand diagnostic tests.
- **non-disruptive**—Starts the non-disruptive test suite.

You can schedule the tests as follows:

- **Daily**—Use the `daily hh:mm` parameter.
- **Specific day and time**—Use the `on mm dd yyyy hh:mm` parameter.
- **Weekly**—Use the `weekly day-of-week hh:mm` parameter.

## Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing on a Switch while it is connected to a live network. You can configure the execution interval for each health-monitoring test, enable the Switch to generate a syslog message because of a test failure, and enable a specific test.

Use the `no` form of this command to disable testing.

By default, health monitoring is disabled, but the Switch generates a syslog message when a test fails.

Follow these steps to configure and enable the health-monitoring diagnostic tests:

### SUMMARY STEPS

1. enable
2. configure terminal
3. diagnostic monitor interval test \{name | test-id | test-id-range | all\} hh:mm:ss milliseconds day
4. diagnostic monitor syslog
5. diagnostic monitor threshold number test \{name | test-id | test-id-range | all\} failure count count
6. diagnostic monitor test \{name | test-id | test-id-range | all\}
7. end
8. show running-config
9. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>diagnostic monitor interval test {name</td>
<td>test-id</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>When specifying the tests, use one of these parameters:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# diagnostic monitor interval test 1 12:30:00 750 5</td>
<td>• name—Name of the test that appears in the show diagnostic content command output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• test-id—ID number of the test that appears in the show diagnostic content command output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• test-id-range—ID numbers of the tests that appear in the show diagnostic content command output.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• all—All of the diagnostic tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When specifying the interval, set these parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• hh:mm:ss—Monitoring interval in hours, minutes, and seconds. The range for hh is 0 to 24, and the range for mm and ss is 0 to 60.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• milliseconds—Monitoring interval in milliseconds (ms). The range is from 0 to 999.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• day—Monitoring interval in the number of days. The range is from 0 to 20.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>diagnostic monitor syslog</td>
<td>(Optional) Configures the switch to generate a syslog message when a health-monitoring test fails.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# diagnostic monitor syslog</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>diagnostic monitor threshold number test {name</td>
<td>test-id</td>
<td>test-id-range</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# diagnostic monitor threshold test 1 failure count 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>diagnostic monitor test {name</td>
<td>test-id</td>
<td>test-id-range</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# diagnostic monitor test 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What to do next

Use the `no diagnostic monitor interval test test-id | test-id-range` global configuration command to change the interval to the default value or to zero. Use the `no diagnostic monitor syslog` command to disable generation of syslog messages when a health-monitoring test fails. Use the `diagnostic monitor threshold test test-id | test-id-range | failure count` command to remove the failure threshold.

Monitoring and Maintaining Online Diagnostics

Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured for the Switch and check the test results by using the privileged EXEC `show` commands in this table:

Table 101: Commands for Diagnostic Test Configuration and Results

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic content</td>
<td>Displays the online diagnostics configured for a switch.</td>
</tr>
<tr>
<td>show diagnostic status</td>
<td>Displays the currently running diagnostic tests.</td>
</tr>
<tr>
<td>show diagnostic result switch [number</td>
<td>all] [detail</td>
</tr>
<tr>
<td>show diagnostic detail]</td>
<td>Displays the online diagnostics test results.</td>
</tr>
<tr>
<td>show diagnostic schedule</td>
<td>Displays the online diagnostics test schedule.</td>
</tr>
<tr>
<td>show diagnostic post</td>
<td>Displays the POST results. (The output is the same as the show post command output.)</td>
</tr>
</tbody>
</table>

Configuration Examples for Online Diagnostic Tests

Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the switch, use the `diagnostic start` privileged EXEC command to begin diagnostic testing.

After starting the tests, you cannot stop the testing process.

Use this privileged EXEC command to manually start online diagnostic testing.
SUMMARY STEPS

1. diagnostic start test \{name | test-id | test-id-range | all | basic | non-disruptive \}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>diagnostic start test {name</td>
<td>test-id</td>
</tr>
</tbody>
</table>

Example:

Switch# diagnostic start test basic

You can specify the tests by using one of these options:

- **name**—Enters the name of the test.
- **test-id**—Enters the ID number of the test.
- **test-id-range**—Enters the range of test IDs by using integers separated by a comma and a hyphen.
- **all**—Starts all of the tests.
- **basic**—Starts the basic test suite.
- **non-disruptive**—Starts the non-disruptive test suite.

Example: Configure a Health Monitoring Test

This example shows how to configure a health-monitoring test:

Switch(config)# diagnostic monitor threshold test 1 failure count 50
Switch(config)# diagnostic monitor interval test TestPortAsicLoopback

**Note**
The Catalyst 2960L switch is not stackable. Hence, the **switch number** keyword is not supported on this switch.

Examples: Schedule Diagnostic Test

This example shows how to schedule diagnostic testing for a specific day and time on a specific switch:

Switch(config)# diagnostic schedule test DiagThermalTest on June 3 2013 22:25

This example shows how to schedule diagnostic testing to occur weekly at a certain time on a specific switch:

Switch(config)# diagnostic schedule switch 1 test 1,2,4-6 weekly saturday 10:30
The Catalyst 2960L switch is not stackable. Hence, the `switch number` keyword is not supported on this switch.

# Displaying Online Diagnostics: Examples

This example shows how to display the online diagnostic detailed information on a switch:

```bash
Switch# show diagnostic switch detail

:  SerialNo :

Overall Diagnostic Result : UNTESTED

Test results: (. = Pass, F = Fail, U = Untested)

1) TestPortAsicLoopback --------------> U
   Error code ------------------------> 3 (DIAG_SKIPPED)
   Total run count ------------------> 0
   Last test testing type ----------> n/a
   Last test execution time -------> n/a
   First test failure time ---------> n/a
   Last test failure time ---------> n/a
   Last test pass time ---------------> n/a
   Total failure count --------------> 0
   Consecutive failure count -------> 0

2) TestPortAsicCam ------------------> U
   Error code ------------------------> 3 (DIAG_SKIPPED)
   Total run count ------------------> 0
   Last test testing type ----------> n/a
   Last test execution time -------> n/a
   First test failure time ---------> n/a
   Last test failure time ---------> n/a
   Last test pass time ---------------> n/a
   Total failure count --------------> 0
   Consecutive failure count -------> 0

3) TestPortAsicMem ------------------> U
   Error code ------------------------> 3 (DIAG_SKIPPED)
   Total run count ------------------> 0
   Last test testing type ----------> n/a
   Last test execution time -------> n/a
   First test failure time ---------> n/a
   Last test failure time ---------> n/a
   Last test pass time ---------------> n/a
   Total failure count --------------> 0
   Consecutive failure count -------> 0
```

This example shows how to display the online diagnostics that are configured on a switch:
Switch# `show diagnostic content`

```
Diagnostics test suite attributes:
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive
R/* - Switch will reload after test list completion / NA
P/* - will partition stack / NA
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Name</th>
<th>Attributes</th>
<th>Test Interval</th>
<th>Thre-day hh:mm:ss.ms shold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TestPortAsicLoopback</td>
<td>B<em>D</em>X**IR*</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>2</td>
<td>TestPortAsicCam</td>
<td>B<em>D</em>X**IR*</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>3</td>
<td>TestPortAsicMem</td>
<td>B<em>D</em>X**IR*</td>
<td>not configured</td>
<td>n/a</td>
</tr>
</tbody>
</table>

This example shows how to display the online diagnostic results for a switch:

Switch# `show diagnostic result`

```
: SerialNo :

Overall Diagnostic Result : UNTESTED

Test results: (. = Pass, F = Fail, U = Untested)

  1) TestPortAsicLoopback ------------> U
  2) TestPortAsicCam -----------------> U
  3) TestPortAsicMem -----------------> U
```

This example shows how to display the online diagnostic test status:

Switch# `show diagnostic status`

```
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics
```

```
---------- ------------------------------- -------------------------------
Card    Description                        Current Running Test Run by
---------- ------------------------------- -------------------------------
          N/A                            N/A
---------- -------------------------------
```

Switch#

This example shows how to display the online diagnostic test schedule for a switch:

Switch# `show diagnostic schedule`

```
Current Time = 17:06:07 IST Tue Sep 11 2018
```

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
Displaying Online Diagnostics: Examples

Diagnostic is not scheduled.
This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the switch. Depending on the nature of the problem, you can use the command-line interface (CLI), Device Manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

- Information About Troubleshooting the Software Configuration, on page 989
- How to Troubleshoot the Software Configuration, on page 996
- Verifying Troubleshooting of the Software Configuration, on page 1010
- Scenarios for Troubleshooting the Software Configuration, on page 1013
- Configuration Examples for Troubleshooting Software, on page 1015
- Additional References for Troubleshooting Software Configuration, on page 1017
- Feature History and Information for Troubleshooting Software Configuration, on page 1018

Information About Troubleshooting the Software Configuration

Software Failure on a Switch

Switch software can be corrupted during an upgrade by downloading the incorrect file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

Related Topics
  Recovering from a Software Failure

Lost or Forgotten Password on a Switch

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.
On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message reminds you to return to the default configuration during the recovery process.

You cannot recover encryption password key, when Cisco WLC configuration is copied from one Cisco WLC to another (in case of an RMA).

**Note**

**Note**

**Power over Ethernet Ports**

A Power over Ethernet (PoE) switch port automatically supplies power to one of these connected devices if the switch detects 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
- an IEEE 802.3at-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.

After the switch detects a powered device, the switch determines the device power requirements and then grants or denies power to the device. The switch can also detect the real-time power consumption of the device by monitoring and policing the power usage.

For more information, see the "Configuring PoE" chapter in the *Catalyst 2960-X Switch Interface and Hardware Component Configuration Guide*.

**Related Topics**

- Recovering from a Lost or Forgotten Password

**Disabled Port Caused by Power Loss**

If a powered device (such as a Cisco IP Phone 7910) that is connected to a PoE Switch port and powered by an AC power source loses power from the AC power source, the device might enter an error-disabled state. To recover from an error-disabled state, enter the `shutdown` interface configuration command, and then enter the `no shutdown` interface command. You can also configure automatic recovery on the Switch to recover from the error-disabled state.

On a Switch, the `errdisable recovery cause loopback` and the `errdisable recovery interval seconds` global configuration commands automatically take the interface out of the error-disabled state after the specified period of time.
Monitoring PoE Port Status

- `show controllers power inline` privileged EXEC command
- `show power inline` EXEC command
- `debug ilpower` privileged EXEC command

Disabled Port Caused by False Link-Up

If a Cisco powered device is connected to a port and you configure the port by using the `power inline never` interface configuration command, a false link-up can occur, placing the port into an error-disabled state. To take the port out of the error-disabled state, enter the `shutdown` and the `no shutdown` interface configuration commands.

You should not connect a Cisco powered device to a port that has been configured with the `power inline never` command.

Ping

The Switch supports IP ping, which you can use to test connectivity to remote hosts. Ping sends an echo request packet to an address and waits for a reply. Ping returns one of these responses:

- Normal response—The normal response (`hostname` is alive) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a `no-answer` message is returned.
- Unknown host—If the host does not exist, an `unknown host` message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a `destination-unreachable` message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a `network or host unreachable` message is returned.

Related Topics
- Executing Ping, on page 1007
- Example: Pinging an IP Host, on page 1015

Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. Layer 2 traceroute supports only unicast source and destination MAC addresses. Traceroute finds the path by using the MAC address tables of the Switch in the path. When the Switch detects a device in the path that does not support Layer 2 traceroute, the Switch continues to send Layer 2 trace queries and lets them time out.

The Switch can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.
Layer 2 Traceroute Guidelines

• Cisco Discovery Protocol (CDP) must be enabled on all the devices in the network. For Layer 2 traceroute to function properly, do not disable CDP.

If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices.

• A Switch is reachable from another Switch when you can test connectivity by using the ping privileged EXEC command. All Switch in the physical path must be reachable from each other.

• The maximum number of hops identified in the path is ten.

• You can enter the traceroute mac or the traceroute mac ip privileged EXEC command on a Switch that is not in the physical path from the source device to the destination device. All Switch in the path must be reachable from this switch.

• The traceroute mac command output shows the Layer 2 path only when the specified source and destination MAC addresses belong to the same VLAN. If you specify source and destination MAC addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

• If you specify a multicast source or destination MAC address, the path is not identified, and an error message appears.

• If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

• The traceroute mac ip command output shows the Layer 2 path when the specified source and destination IP addresses belong to the same subnet. When you specify the IP addresses, the Switch uses the Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

  • If an ARP entry exists for the specified IP address, the Switch uses the associated MAC address and identifies the physical path.

  • If an ARP entry does not exist, the Switch sends an ARP query and tries to resolve the IP address. If the IP address is not resolved, the path is not identified, and an error message appears.

• When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute feature is not supported. When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

• This feature is not supported in Token Ring VLANs.

IP Traceroute

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Your Switch can participate as the source or destination of the traceroute privileged EXEC command and might or might not appear as a hop in the traceroute command output. If the Switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate Switch do not show up in the traceroute output if they are only bridging the packet from one port to another within the same VLAN.
However, if the intermediate Switch is a multilayer Switch that is routing a particular packet, this Switch shows up as a hop in the traceroute output.

The **traceroute** privileged EXEC command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends an Internet Control Message Protocol (ICMP) time-to-live-exceeded message to the sender. Traceroute finds the address of the first hop by examining the source address field of the ICMP time-to-live-exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To learn when a datagram reaches its destination, traceroute sets the UDP destination port number in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram destined to itself containing a destination port number that is unused locally, it sends an ICMP `port-unreachable` error to the source. Because all errors except port-unreachable errors come from intermediate hops, the receipt of a port-unreachable error means that this message was sent by the destination port.

**Related Topics**

- Executing IP Traceroute, on page 1008
- Example: Performing a Traceroute to an IP Host, on page 1016

**Time Domain Reflector Guidelines**

You can use the Time Domain Reflector (TDR) feature to diagnose and resolve cabling problems. When running TDR, a local device sends a signal through a cable and compares the reflected signal to the initial signal.

TDR is supported only on 10/100/1000 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and on SFP module ports.

TDR can detect these cabling problems:

- Open, broken, or cut twisted-pair wires—The wires are not connected to the wires from the remote device.
- Shorted twisted-pair wires—The wires are touching each other or the wires from the remote device. For example, a shorted twisted pair can occur if one wire of the twisted pair is soldered to the other wire.

  If one of the twisted-pair wires is open, TDR can find the length at which the wire is open.

Use TDR to diagnose and resolve cabling problems in these situations:

- Replacing a Switch
- Setting up a wiring closet
- Troubleshooting a connection between two devices when a link cannot be established or when it is not operating properly

When you run TDR, the Switch reports accurate information in these situations:
• The cable for the gigabit link is a solid-core cable.
• The open-ended cable is not terminated.

When you run TDR, the Switch does not report accurate information in these situations:
• The cable for the gigabit link is a twisted-pair cable or is in series with a solid-core cable.
• The link is a 10-megabit or a 100-megabit link.
• The cable is a stranded cable.
• The link partner is a Cisco IP Phone.
• The link partner is not IEEE 802.3 compliant.

### Debug Commands

⚠️ **Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use `debug` commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use `debug` commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased `debug` command processing overhead will affect system use.

All `debug` commands are entered in privileged EXEC mode, and most `debug` commands take no arguments.

**Related Topics**

- [Redirecting Debug and Error Message Output](#), on page 1009
- [Example: Enabling All System Diagnostics](#), on page 1017

### Onboard Failure Logging on the Switch

You can use the onboard failure logging (OBFL) feature to collect information about the Switch. The information includes uptime, temperature, and voltage information and helps Cisco technical support representatives to troubleshoot Switch problems. We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

By default, OBFL is enabled. It collects information about the Switch and small form-factor pluggable (SFP) modules. The Switch stores this information in the flash memory:

• CLI commands—Record of the OBFL CLI commands that are entered on a standalone Switch or a switch stack member.
• Environment data—Unique device identifier (UDI) information for a standalone Switch or a switch stack member and for all the connected FRU devices: the product identification (PID), the version identification (VID), and the serial number.
• Message—Record of the hardware-related system messages generated by a standalone Switch or a switch stack member.
• Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone Switch or a switch stack member.
- Temperature—Temperature of a standalone Switch or a switch stack member.
- Uptime data—Time when a standalone Switch or a switch stack member starts, the reason the Switch restarts, and the length of time the Switch has been running since it last restarted.
- Voltage—System voltages of a standalone Switch or a switch stack member.

You should manually set the system clock or configure it by using Network Time Protocol (NTP).

When the Switch is running, you can retrieve the OBFL data by using the `show logging onboard` privileged EXEC commands. If the Switch fails, contact your Cisco technical support representative to find out how to retrieve the data.

When an OBFL-enabled Switch is restarted, there is a 10-minute delay before logging of new data begins.

**Related Topics**
- Configuring OBFL, on page 1010
- Displaying OBFL Information

## Possible Symptoms of High CPU Utilization

Excessive CPU utilization might result in these symptoms, but the symptoms might also result from other causes:

### Note
You may see increased system memory usage when Cisco Catalyst 4500E Supervisor Engine 8-E is used in wireless mode.

- Spanning tree topology changes
- EtherChannel links brought down due to loss of communication
- Failure to respond to management requests (ICMP ping, SNMP timeouts, slow Telnet or SSH sessions)
- UDLD flapping
- IP SLAs failures because of SLAs responses beyond an acceptable threshold
- DHCP or IEEE 802.1x failures if the switch does not forward or respond to requests

Layer 3 switches:
- Dropped packets or increased latency for packets routed in software
- BGP or OSPF routing topology changes
How to Troubleshoot the Software Configuration

Recovering from a Software Failure

Switch software can be corrupted during an upgrade by downloading the wrong file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

This procedure uses the Xmodem Protocol to recover from a corrupt or wrong image file. There are many software packages that support the Xmodem Protocol, and this procedure is largely dependent on the emulation software that you are using.

This recovery procedure requires that you have physical access to the switch.

---

**Step 1**
From your PC, download the software image tar file (image_filename.tar) from Cisco.com. The Cisco IOS image is stored as a bin file in a directory in the tar file. For information about locating the software image files on Cisco.com, see the release notes.

**Step 2**
Extract the bin file from the tar file. If you are using Windows, use a zip program that can read a tar file. Use the zip program to navigate. If you are using Windows, use a zip program that can read a tar file. Use the zip program to navigate. If you are using UNIX, follow these steps:

a) Display the contents of the tar file by using the `tar -tvf <image_filename.tar>` UNIX command.

   **Example:**
   ```
   unix-1% tar -tvf image_filename.tar
   ```

b) Locate the bin file, and extract it by using the `tar -xvf <image_filename.tar> <image_filename.bin>` UNIX command.

   **Example:**
   ```
   unix-1% tar -xvf image_filename.tar image_filename.bin
   x c2960x-universalk9-mz-150-2.EX1/c2960x-universalk9-mz-150-2.EX1.bin, 2928176 bytes, 5720 tape blocks
   ```

c) Verify that the bin file was extracted by using the `ls -l <image_filename.bin>` UNIX command.

   **Example:**
   ```
   unix-1% ls -l image_filename.bin
   -rw-r--r-- 1 boba 2928176 Apr 21 12:01 c2960x-universalk9-mz.150-2.0.66.ucp/c2960x-universalk9-mz.150-2.0.66.ucp.bin
   ```

**Step 3**
Connect your PC with terminal-emulation software supporting the Xmodem Protocol to the switch console port.

**Step 4**
Set the line speed on the emulation software to 9600 baud.

**Step 5**
Unplug the switch power cord.

**Step 6**
Press the Mode button, and at the same time reconnect the power cord to the switch. You can release the Mode button a second or two after the LED above port 1 goes off. Several lines of information about the software appear along with instructions.

**Example:**
The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software:

```
flash_init
load_helper
boot
```

**Step 7** Initialize the flash file system.

**Example:**
```
switch: flash_init
```

**Step 8** If you had set the console port speed to any speed other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

**Step 9** Load any helper files.

**Example:**
```
switch: load_helper
```

**Step 10** Start the file transfer by using the Xmodem Protocol.

**Example:**
```
switch: copy xmodem: flash:image_filename.bin
```

**Step 11** After the Xmodem request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image into flash memory.

**Step 12** Boot the newly downloaded Cisco IOS image.

**Example:**
```
switch: boot flash:image_filename.bin
```

**Step 13** Use the `archive download-sw` privileged EXEC command to download the software image to the switch.

**Step 14** Use the `reload` privileged EXEC command to restart the switch and to verify that the new software image is operating properly.

**Step 15** Delete the `flash:image_filename.bin` file from the switch.

---

**Recovering from a Lost or Forgotten Password**

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.
On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

You enable or disable password recovery by using the `service password-recovery` global configuration command.

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.

**Note**

You enable or disable password recovery by using the `service password-recovery` global configuration command.

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.

---

**Step 1** Connect a terminal or PC to the switch.
- Connect a terminal or a PC with terminal-emulation software to the switch console port.
  
  **Or**
  
  Connect a PC to the Ethernet management port.

**Step 2** Set the line speed on the emulation software to 9600 baud.

**Step 3** On a switch, power off the switch.

**Step 4** Reconnect the power cord to the switch. Within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until all the system LEDs turn on and remain solid, then release the **Mode** button.

Several lines of information about the software appear with instructions, informing you if the password recovery procedure has been disabled or not.

- If you see a message that begins with this statement:
  
  The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system

  proceed to the "Procedure with Password Recovery Enabled" section, and follow the steps.

- If you see a message that begins with this statement:
  
  The password-recovery mechanism has been triggered, but is currently disabled.

  proceed to the "Procedure with Password Recovery Disabled" section, and follow the steps.

**Step 5** After recovering the password, reload the switch.

On a switch:

```
Switch> reload
Proceed with reload? [confirm] y
```
Procedure with Password Recovery Enabled

If the password-recovery operation is enabled, this message appears:

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software:

`flash_init`
`load_helper`
`boot`

---

**Step 1** Initializethe flash file system.

Switch: `flash_init`

**Step 2** If you had set the console port speed to any number other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

**Step 3** Load any helper files.

Switch: `load_helper`

**Step 4** Display the contents of flash memory.

Switch: `dir: flash:
Directory of flash:
  11 -rw x 5825 Mar 01 2013 22:31:59 config.text

16128000 bytes total (10003456 bytes free)`

**Step 5** Rename the configuration file to `config.text.old` This file contains the password definition.

Switch: `rename flash: config.text flash: config.text.old`

**Step 6** Boot up the system.

Switch: `boot`

You are prompted to start the setup program. Enter N at the prompt.

Continue with the configuration dialog?? [yes/no]: No

**Step 7** At the switch prompt, enter privileged EXEC mode.

Switch> `enable`
Switch#

**Step 8** Rename the configuration file to its original name.

Switch# `rename flash: config.text.old flash: config.text`
Step 9  Copy the configuration file into memory

Switch# copy flash: config.text system: running-config
Source filename [config.text]?
Destination filename [running-config]?

Press Return in response to the confirmation prompts. The configuration file is now reloaded, and you can change the password.

Step 10 Enter global configuration mode.

Switch# configure terminal

Step 11 Change the password.

Switch(config)# enable secret password

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 12 Return to privileged EXEC mode.

Switch(config)# exit
Switch#

Step 13 Write the running configuration to the startup configuration file.

Switch# copy running-config startup-config

The new password is now in the startup configuration.

Note  This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the show running-config privileged EXEC command. To reenable the interface, enter the interface vlan vlan-id global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the no shutdown command.

Step 14 Boot the switch with the packages.conf file from flash.

Switch: boot flash:packages.conf

Step 15 Reload the switch.

Switch# reload

---

Procedure with Password Recovery Disabled

If the password-recovery mechanism is disabled, this message appears:

The password-recovery mechanism has been triggered, but is currently disabled. Access to the boot loader prompt through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be reset back to the default system configuration, access to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?

⚠️ Caution
Returning the Switch to the default configuration results in the loss of all existing configurations. We recommend that you contact your system administrator to verify if there are backup Switch and VLAN configuration files.

- If you enter n (no), the normal boot process continues as if the Mode button had not been pressed; you cannot access the boot loader prompt, and you cannot enter a new password. You see the message:

  Press Enter to continue........

- If you enter y (yes), the configuration file in flash memory and the VLAN database file are deleted. When the default configuration loads, you can reset the password.

---

**Step 1** Choose to continue with password recovery and delete the existing configuration:

Would you like to reset the system back to the default configuration (y/n)? Y

**Step 2** Display the contents of flash memory:

Switch: `dir flash`:

The Switch filesystem appears.

```
Directory of flash:
  13 drwx 192 Mar 01 2013 22:30:48 c2960x-universalk9-mz.150-2.0.63.UCP.bin
  16128000 bytes total (10003456 bytes free)
```

**Step 3** Boot up the system:

Switch: `boot`

You are prompted to start the setup program. To continue with password recovery, enter N at the prompt:

Continue with the configuration dialog? [yes/no]: N

**Step 4** At the Switch prompt, enter privileged EXEC mode:

Switch> `enable`

**Step 5** Enter global configuration mode:
Switch# configure terminal

Step 6  Change the password:
Switch(config)# enable secret password

The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 7  Return to privileged EXEC mode:
Switch(config)# exit
Switch#

Note  Before continuing to Step 9, power on any connected stack members and wait until they have completely initialized. The stacking feature is supported on Switch running the LAN Base image.

Step 8  Write the running configuration to the startup configuration file:
Switch# copy running-config startup-config

The new password is now in the startup configuration.

Step 9  You must now reconfigure the Switch. If the system administrator has the backup Switch and VLAN configuration files available, you should use those.

---

Recovering from a Command Switch Failure

If you have not configured a standby command switch, and your command switch loses power or fails in some other way, management contact with the member switches is lost, and you must install a new command switch. However, connectivity between switches that are still connected is not affected, and the member switches forward packets as usual. You can manage the members as stand-alone switches through the console port, or, if they have IP addresses, through the other management interfaces.

You can prepare for a command switch failure by assigning an IP address to a member switch or another switch that is command-capable, making a note of the command-switch password, and cabling your cluster to provide redundant connectivity between the member switches and the replacement command switch. These sections describe two solutions for replacing a failed command switch:

• Replacing a Failed Command Switch with a Cluster Member

• Replacing a Failed Command Switch with Another Switch

These recovery procedures require that you have physical access to the switch. For information on command-capable switches, see the release notes.

Replacing a Failed Command Switch with a Cluster Member

To replace a failed command switch with a command-capable member in the same cluster, follow these steps
Step 1
Disconnect the command switch from the member switches, and physically remove it from the cluster.

Step 2
Insert the member switch in place of the failed command switch, and duplicate its connections to the cluster members.

Step 3
Start a CLI session on the new command switch.

You can access the CLI by using the console port or, if an IP address has been assigned to the switch, by using Telnet. For details about using the console port, see Catalyst 2960-X Switch Hardware Installation Guide.

Step 4
At the switch prompt, enter privileged EXEC mode.

Example:
```
Switch> enable
Switch#
```

Step 5
Enter the password of the failed command switch.

Step 6
Enter global configuration mode.

Example:
```
Switch# configure terminal
```
Enter configuration commands, one per line. End with CNTL/Z.

Step 7
Remove the member switch from the cluster.

Example:
```
Switch(config)# no cluster commander-address
```

Step 8
Return to privileged EXEC mode.

Example:
```
Switch(config)# end
Switch#
```

Step 9
Use the setup program to configure the switch IP information. This program prompts you for IP address information and passwords. From privileged EXEC mode, enter EXEC mode, enter `setup`, and press `Return`.

Example:
```
Switch# setup
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '{}'.
Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system.
Would you like to enter basic management setup? [yes/no]:
```

Step 10
Enter `Y` at the first prompt.

Example:
```
The prompts in the setup program vary depending on the member switch that you selected to be the command switch:
Continue with configuration dialog? [yes/no]: y
Configuring global parameters:

If this prompt does not appear, enter enable, and press Return. Enter setup, and press Return to start the setup program.

Step 11 Respond to the questions in the setup program.

When prompted for the hostname, it is limited to 28 characters and 31 characters on a member switch. Do not use -n, where n is a number, as the last characters in a hostname for any switch. When prompted for the Telnet (virtual terminal) password, it is 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 12 When prompted for the enable secret and enable passwords, enter the passwords of the failed command switch again.

Step 13 When prompted, make sure to enable the switch as the cluster command switch, and press Return.

Step 14 When prompted, assign a name to the cluster, and press Return.

The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

Step 15 After the initial configuration displays, verify that the addresses are correct.

Step 16 If the displayed information is correct, enter Y, and press Return.

If this information is not correct, enter N, press Return, and begin again at Step 9.

Step 17 Start your browser, and enter the IP address of the new command switch.

Step 18 From the Cluster menu, select Add to Cluster to display a list of candidate switches to add to the cluster.

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system.
Would you like to enter basic management setup? [yes/no]:

**Step 6**
Enter Y at the first prompt.

**Example:**

The prompts in the setup program vary depending on the member switch that you selected to be the command switch:
Continue with configuration dialog? [yes/no]: Y

or

Configuring global parameters:

If this prompt does not appear, enter enable, and press Return. Enter setup, and press Return to start the setup program.

**Step 7**
Respond to the questions in the setup program.

When prompted for the hostname, it is limited to 28 characters and 31 characters on a member switch. Do not use -n, where n is a number, as the last characters in a hostname for any switch. When prompted for the Telnet (virtual terminal) password, it is 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

**Step 8**
When prompted for the enable secret and enable passwords, enter the passwords of the failed command switch again.

**Step 9**
When prompted, make sure to enable the switch as the cluster command switch, and press Return.

**Step 10**
When prompted, assign a name to the cluster, and press Return.

The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

**Step 11**
After the initial configuration displays, verify that the addresses are correct.

**Step 12**
If the displayed information is correct, enter Y, and press Return.

If this information is not correct, enter N, press Return, and begin again at Step 9.

**Step 13**
Start your browser, and enter the IP address of the new command switch.

**Step 14**
From the Cluster menu, select Add to Cluster to display a list of candidate switches to add to the cluster.

---

**Preventing Switch Stack Problems**

To prevent switch stack problems, you should do the following:

- Make sure that the Switch that you add to or remove from the switch stack are powered off. For all powering considerations in switch stacks, see the “Switch Installation” chapter in the hardware installation guide.

- Press the Mode button on a stack member until the Stack mode LED is on. The last two port LEDs on the Switch should be green. Depending on the Switch model, the last two ports are either 10/100/1000 ports or small form-factor pluggable (SFP) module. If one or both of the last two port LEDs are not green, the stack is not operating at full bandwidth.
• We recommend using only one CLI session when managing the switch stack. Be careful when using multiple CLI sessions to the active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible that you might not be able to identify the session from which you entered a command.

• Manually assigning stack member numbers according to the placement of the Switch in the stack can make it easier to remotely troubleshoot the switch stack. However, you need to remember that the Switch have manually assigned numbers if you add, remove, or rearrange Switch later. Use the `switch current-stack-member-number renumber new-stack-member-number` global configuration command to manually assign a stack member number.

If you replace a stack member with an identical model, the new Switch functions with the exact same configuration as the replaced Switch. This is also assuming the new Switch is using the same member number as the replaced Switch.

Removing powered-on stack members causes the switch stack to divide (partition) into two or more switch stacks, each with the same configuration. If you want the switch stacks to remain separate, change the IP address or addresses of the newly created switch stacks. To recover from a partitioned switch stack, follow these steps:

1. Power off the newly created switch stacks.
2. Reconnect them to the original switch stack through their StackWise Plus ports.
3. Power on the Switch.

For the commands that you can use to monitor the switch stack and its members, see the `Displaying Switch Stack Information` section.

Preventing Autonegotiation Mismatches

The IEEE 802.3ab autonegotiation protocol manages the Switch settings for speed (10 Mb/s, 100 Mb/s, and 1000 Mb/s, excluding SFP module ports) and duplex (half or full). There are situations when this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

• A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.

• A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize Switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

• Let both ports autonegotiate both speed and duplex.

• Manually set the speed and duplex parameters for the ports on both ends of the connection.

**Note**

If a remote device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate.
Troubleshooting SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the Switch, the Switch software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note
The security error message references the GBIC_SECURITY facility. The Switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces.

If you are using a non-Cisco SFP module, remove the SFP module from the Switch, and replace it with a Cisco module. After inserting a Cisco SFP module, use the `errdisable recovery cause gbic-invalid` global configuration command to verify the port status, and enter a time interval for recovering from the error-disabled state. After the elapsed interval, the Switch brings the interface out of the error-disabled state and retries the operation. For more information about the `errdisable recovery` command, see the command reference for this release.

If the module is identified as a Cisco SFP module, but the system is unable to read vendor-data information to verify its accuracy, an SFP module error message is generated. In this case, you should remove and reinsert the SFP module. If it continues to fail, the SFP module might be defective.

Monitoring SFP Module Status

You can check the physical or operational status of an SFP module by using the `show interfaces transceiver` privileged EXEC command. This command shows the operational status, such as the temperature and the current for an SFP module on a specific interface and the alarm status. You can also use the command to check the speed and the duplex settings on an SFP module. For more information, see the `show interfaces transceiver` command in the command reference for this release.

Executing Ping

If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or have IP routing configured to route between those subnets.

IP routing is disabled by default on all Switch.

Note
Though other protocol keywords are available with the `ping` command, they are not supported in this release.

Use this command to ping another device on the network from the Switch:
### Monitoring Temperature

The Switch monitors the temperature conditions and uses the temperature information to control the fans.

Use the `show env temperature status` privileged EXEC command to display the temperature value, state, and thresholds. The temperature value is the temperature in the Switch (not the external temperature). You can configure only the yellow threshold level (in Celsius) by using the `system env temperature threshold yellow value` global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds. For more information, see the command reference for this release.

### Monitoring the Physical Path

You can monitor the physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tracert route mac [interface interface-id] (source-mac-address) [interface interface-id] (destination-mac-address) [vlan vlan-id] [detail]</code></td>
<td>Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.</td>
</tr>
<tr>
<td>`tracert route mac ip (source-ip-address</td>
<td>source-hostname) (destination-ip-address</td>
</tr>
</tbody>
</table>

### Executing IP Traceroute

Though other protocol keywords are available with the `tracert route` privileged EXEC command, they are not supported in this release.
### Running TDR and Displaying the Results

When you run TDR on an interface, you can run it on the active switch or a stack member.

To run TDR, enter the `test cable-diagnostics tdr interface interface-id` privileged EXEC command.

To display the results, enter the `show cable-diagnostics tdr interface interface-id` privileged EXEC command.

### Redirecting Debug and Error Message Output

By default, the network server sends the output from `debug` commands and system error messages to the console. If you use this default, you can use a virtual terminal connection to monitor debug output instead of connecting to the console port or the Ethernet management port.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

---

**Note**

Be aware that the debugging destination you use affects system overhead. When you log messages to the console, very high overhead occurs. When you log messages to a virtual terminal, less overhead occurs. Logging messages to a syslog server produces even less, and logging to an internal buffer produces the least overhead of any method.

For more information about system message logging, see *Configuring System Message Logging*.

### Using the `show platform forward` Command

The output from the `show platform forward` privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

Most of the information in the output from the command is useful mainly for technical support personnel, who have access to detailed information about the Switch application-specific integrated circuits (ASICs). However, packet forwarding information can also be helpful in troubleshooting.
Configuring OBFL

**Caution**

We recommend that you do not disable OBFL and that you do not remove the data stored in the flash memory.

- To enable OBFL, use the `hw-switch switch [switch-number] logging onboard [message level level]` global configuration command. On switches, the range for `switch-number` is from 1 to 9. Use the `message level level` parameter to specify the severity of the hardware-related messages that the switch generates and stores in the flash memory.

- To copy the OBFL data to the local network or a specific file system, use the `copy onboard switch switch-number url url-destination` privileged EXEC command.

- To disable OBFL, use the `no hw-switch switch [switch-number] logging onboard [message level level]` global configuration command.

- To clear all the OBFL data in the flash memory except for the uptime and CLI command information, use the `clear onboard switch switch-number` privileged EXEC command.

- In a switch stack, you can enable OBFL on a standalone switch or on all stack members by using the `hw-switch switch [switch-number] logging onboard [message level level]` global configuration command.

- You can enable or disable OBFL on a member switch from the active switch.

For more information about the commands in this section, see the command reference for this release.

**Related Topics**

- Onboard Failure Logging on the Switch, on page 994
- Displaying OBFL Information

Verifying Troubleshooting of the Software Configuration

Displaying OBFL Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging onboard [module[switch-number ]]clilog</code>&lt;br&gt;Switch# show logging onboard 1 clilog</td>
<td>Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members.</td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] environment</code>&lt;br&gt;Switch# show logging onboard 1 environment</td>
<td>Displays the UDI information for a standalone switch or the specified stack members and for all the connected FRU devices: the PID, the VID, and the serial number.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **show logging onboard [module[switch-number ]]] message**  
Switch# show logging onboard 1 message | Displays the hardware-related messages generated by a standalone switch or the specified stack members. |
| **show logging onboard [module[switch-number ]]] poe**  
Switch# show logging onboard 1 poe | Displays the power consumption of PoE ports on a standalone switch or the specified stack members. |
| **show logging onboard [module[switch-number ]]] temperature**  
Switch# show logging onboard 1 temperature | Displays the temperature of a standalone switch or or the specified stack members. |
| **show logging onboard [module[switch-number ]]] uptime**  
Switch# show logging onboard 1 uptime | Displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or specified stack members restart, and the length of time that the standalone switch or the specified stack members have been running since they last restarted. |
| **show logging onboard [module[switch-number ]]] voltage**  
Switch# show logging onboard 1 voltage | Displays the system voltages of a standalone switch or the specified stack members. |
| **show logging onboard [module[switch-number ]]] continuous**  
Switch# show logging onboard 1 continuous | Displays the data in the continuous file. |
| **show logging onboard [module[switch-number ]]] detail**  
Switch# show logging onboard 1 detail | Displays both the continuous and summary data . |
| **show logging onboard [module[switch-number ]]] endhh:mm:ss**  
Switch# show logging onboard 1  
end 13:00:15 jul 2013 | Displays end time and date on a standalone switch or the specified stack members. |
| **show logging onboard [module[switch-number ]]]**  
Switch# show logging onboard 1 | Displays OBFL information about the specified switches in the system. |
| **show logging onboard [module[switch-number ]]] raw**  
Switch# show logging onboard 1 raw | Displays the raw information on a standalone switch or the specified stack members. |
Example: Verifying the Problem and Cause for High CPU Utilization

To determine if high CPU utilization is a problem, enter the `show processes cpu sorted` privileged EXEC command. Note the underlined information in the first line of the output example.

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...<output truncated>
```

This example shows normal CPU utilization. The output shows that utilization for the last 5 seconds is 8%/0%, which has this meaning:

- The total CPU utilization is 8 percent, including both time running Cisco IOS processes and time spent handling interrupts.
- The time spent handling interrupts is zero percent.

### Table 104: Troubleshooting CPU Utilization Problems

<table>
<thead>
<tr>
<th>Type of Problem</th>
<th>Cause</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interrupt percentage value is almost as high as total CPU utilization value.</td>
<td>The CPU is receiving too many packets from the network.</td>
<td>Determine the source of the network packet. Stop the flow, or change the switch configuration. See the section on “Analyzing Network Traffic.”</td>
</tr>
</tbody>
</table>
Corrective Action

<table>
<thead>
<tr>
<th>Type of Problem</th>
<th>Cause</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total CPU utilization is greater than 50% with minimal time spent on interrupts.</td>
<td>One or more Cisco IOS process is consuming too much CPU time. This is usually triggered by an event that activated the process.</td>
<td>Identify the unusual event, and troubleshoot the root cause. See the section on “Debugging Active Processes.”</td>
</tr>
</tbody>
</table>

Scenarios for Troubleshooting the Software Configuration

Scenarios to Troubleshoot Power over Ethernet (PoE)

Table 105: Power over Ethernet Troubleshooting Scenarios

<table>
<thead>
<tr>
<th>Symptom or Problem</th>
<th>Possible Cause and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only one port does not have PoE. Trouble is on only one switch port. PoE and non-PoE devices do not work on this port, but do on other ports.</td>
<td>Verify that the powered device works on another PoE port. Use the <code>show run</code>, or <code>show interface status</code> user EXEC commands to verify that the port is not shut down or error-disabled. <strong>Note</strong> Most switches turn off port power when the port is shut down, even though the IEEE specifications make this optional. Verify that the Ethernet cable from the powered device to the switch port is good: Connect a known good non-PoE Ethernet device to the Ethernet cable, and make sure that the powered device establishes a link and exchanges traffic with another host. Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters. Disconnect the Ethernet cable from the switch port. Use a short Ethernet cable to connect a known good Ethernet device directly to this port on the switch front panel (not on a patch panel). Verify that it can establish an Ethernet link and exchange traffic with another host, or ping the port VLAN SVI. Next, connect a powered device to this port, and verify that it powers on. If a powered device does not power on when connected with a patch cord to the switch port, compare the total number of connected powered devices to the switch power budget (available PoE). Use the <code>show inline power</code> command to verify the amount of available power.</td>
</tr>
<tr>
<td>Symptom or Problem</td>
<td>Possible Cause and Solution</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>No PoE on all ports or a group of ports. Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.</td>
<td>If there is a continuous, intermittent, or reoccurring alarm related to power, replace the power supply if possible it is a field-replaceable unit. Otherwise, replace the switch. If the problem is on a consecutive group of ports but not all ports, the power supply is probably not defective, and the problem could be related to PoE regulators in the switch. Use the <code>show log</code> privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes. If there are no alarms, use the <code>show interface status</code> command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the <code>shut</code> and <code>no shut</code> interface configuration commands to reenable the ports. Use the <code>show env power</code> and <code>show power inline</code> privileged EXEC commands to review the PoE status and power budget (available PoE). Review the running configuration to verify that <code>power inline never</code> is not configured on the ports. Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch cord. Do not use the existing distribution cables. Enter the <code>shut</code> and <code>no shut</code> interface configuration commands, and verify that an Ethernet link is established. If this connection is good, use a short patch cord to connect a powered device to this port and verify that it powers on. If the device powers on, verify that all intermediate patch panels are correctly connected. Disconnect all but one of the Ethernet cables from switch ports. Using a short patch cord, connect a powered device to only one PoE port. Verify the powered device does not require more power than can be delivered by the switch port. Use the <code>show power inline</code> privileged EXEC command to verify that the powered device can receive power when the port is not shut down. Alternatively, watch the powered device to verify that it powers on. If a powered device can power on when only one powered device is connected to the switch, enter the <code>shut</code> and <code>no shut</code> interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the <code>show interface status</code> and <code>show power inline</code> privileged EXEC commands to monitor inline power statistics and port status. If there is still no PoE at any port, a fuse might be open in the PoE section of the power supply. This normally produces an alarm. Check the log again for alarms reported earlier by system messages.</td>
</tr>
</tbody>
</table>
## Symptom or Problem

<table>
<thead>
<tr>
<th>Symptom or Problem</th>
<th>Possible Cause and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Phone disconnects or resets. After working normally, a Cisco phone or wireless access point intermittently reloads or disconnects from PoE.</td>
<td>Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads. Verify that the cable length is not more than 100 meters from the switch port to the powered device. Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs. Notice whether any error messages appear at the same time a disconnect occurs. Use the <code>show log</code> privileged EXEC command to review error messages. Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.) Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device.</td>
</tr>
<tr>
<td>Non-Cisco powered device does not work on Cisco PoE switch. A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.</td>
<td>Use the <code>show power inline</code> command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected. Verify that sufficient power is available for the powered device type before you connect it. Use the <code>show interface status</code> command to verify that the switch detects the connected powered device. Use the <code>show log</code> command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or <code>inrush</code>) current that exceeds a current-limit threshold for the port.</td>
</tr>
</tbody>
</table>

### Related Topics

- Power over Ethernet Ports, on page 990

## Configuration Examples for Troubleshooting Software

### Example: Pinging an IP Host

This example shows how to ping an IP host:

```
Switch# ping 172.20.52.3
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#

Table 106: Ping Output Display Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point means receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period means the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error PDU was received.</td>
</tr>
<tr>
<td>C</td>
<td>A congestion experienced packet was received.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

To end a ping session, enter the escape sequence (Ctrl-^ X by default). Simultaneously press and release the Ctrl, Shift, and 6 keys and then press the X key.

Related Topics

- Ping, on page 991
- Executing Ping, on page 1007

Example: Performing a Traceroute to an IP Host

This example shows how to perform a traceroute to an IP host:

Switch# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

1 192.0.2.1 0 msec 0 msec 4 msec
2 192.0.2.203 12 msec 8 msec 0 msec
3 192.0.2.100 4 msec 0 msec 0 msec
4 192.0.2.10 0 msec 4 msec 0 msec

The display shows the hop count, the IP address of the router, and the round-trip time in milliseconds for each of the three probes that are sent.

Table 107: Traceroute Output Display Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The probe timed out.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>Character</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>A</td>
<td>Administratively unreachable. Usually, this output means that an access list is blocking traffic.</td>
</tr>
<tr>
<td>H</td>
<td>Host unreachable.</td>
</tr>
<tr>
<td>N</td>
<td>Network unreachable.</td>
</tr>
<tr>
<td>P</td>
<td>Protocol unreachable.</td>
</tr>
<tr>
<td>Q</td>
<td>Source quench.</td>
</tr>
<tr>
<td>U</td>
<td>Port unreachable.</td>
</tr>
</tbody>
</table>

To end a trace in progress, enter the escape sequence (\texttt{Ctrl-\textasciicircum} X by default). Simultaneously press and release the \texttt{Ctrl}, \texttt{Shift}, and \texttt{6} keys and then press the \texttt{X} key.

**Related Topics**
- IP Traceroute, on page 992
- Executing IP Traceroute, on page 1008

**Example: Enabling All System Diagnostics**

⚠️ **Caution**
Because debugging output takes priority over other network traffic, and because the \texttt{debug all} privileged EXEC command generates more output than any other \texttt{debug} command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific \texttt{debug} commands.

This command disables all-system diagnostics:

\texttt{Switch# debug all}

The \texttt{no debug all} privileged EXEC command disables all diagnostic output. Using the \texttt{no debug all} command is a convenient way to ensure that you have not accidentally left any \texttt{debug} commands enabled.

**Related Topics**
- Debug Commands, on page 994

**Additional References for Troubleshooting Software Configuration**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting commands</td>
<td>Catalyst 2960-X Switch System Management Command Reference</td>
</tr>
</tbody>
</table>
### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

### Feature History and Information for Troubleshooting Software Configuration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
PART XI

Working with the Cisco IOS File System, Configuration Files, and Software Images

• Working with the Cisco IOS File System, Configuration Files, and Software Images, on page 1021
Working with the Cisco IOS File System, Configuration Files, and Software Images

• Working with the Flash File System, on page 1021
• Working with Configuration Files, on page 1030
• Replacing and Rolling Back Configurations, on page 1042
• Working with Software Images , on page 1046
• Copying Image Files Using TFTP, on page 1048
• Copying Image Files Using FTP, on page 1052
• Copying Image Files Using RCP, on page 1056

Working with the Flash File System

Information About the Flash File System

The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software bundles and configuration files. The default flash file system on the switch is named flash:.

As viewed from the active switch, flash: refers to the local flash device, which is the device attached to the same switch on which the file system is being viewed.

Only one user at a time can manage the software bundles and configuration files .

Displaying Available File Systems

To display the available file systems on your switch, use the show file systems privileged EXEC command as shown in this example for a standalone switch:

```
Switch# show file systems
File Systems:
  Size(b)   Free(b)   Type   Flags   Prefixes
  * 15998976   5135872   flash   rw     flash:
    -         -      opaque   rw     bs:
    -         -      opaque   rw     vb:
  524288     520138   nvram   rw     nvram:
    -         -      network  rw     tftp:
```
This example shows a switch stack. In this example, the active switch is stack member 1; the file system on stack member 2 is displayed as flash-2:; the file system on stack member 3 is displayed as flash-3: and so on up to . The example also shows the crashinfo directories and a USB flash drive plugged into the active switch:

```
Switch# show file systems
File Systems:
Size(b) Free(b) Type Flags Prefixes
145894946 5479424 disk rw crashinfo:crashinfo-1:
248512512 85983232 disk rw crashinfo-2:stby-crashinfo:
146014208 17301504 disk rw crashinfo-3:
146014208 0 disk rw crashinfo-4:
146014208 1572864 disk rw crashinfo-5:
248512512 30932992 disk rw crashinfo-6:
146014208 6291456 disk rw crashinfo-7:
146276352 1572864 disk rw crashinfo-8:
146276352 7340032 disk rw crashinfo-9:
* 741621760 481730560 disk rw flash:flash-1:
1622147072 1360527360 disk rw flash-2:stby-flash:
729546752 469762048 disk rw flash-3:
729546752 469762048 disk rw flash-4:
729546752 469762048 disk rw flash-5:
1622147072 1340604416 disk rw flash-6:
729546752 469762048 disk rw flash-7:
1749549056 1487929344 disk rw flash-8:
1749549056 1487929344 disk rw flash-9:
0 0 disk rw unix:
- - disk rw usbflash0:usbflash0-1:
- - disk rw usbflash0-2: stby-usbflash0:
- - disk rw usbflash0-3:
- - disk rw usbflash0-4:
- - disk rw usbflash0-5:
- - disk rw usbflash0-6:
- - disk rw usbflash0-7:
- - disk rw usbflash0-8:
- - disk rw usbflash0-9:
0 0 disk ro webui:
- - opaque rw system:
- - opaque rw tmpsys:
2097152 2055643 nvram rw stby-nvram:
- - nvram rw stby-rcsf:
- - opaque rw null:
- - opaque ro tar:
- - network rw tftp:
2097152 2055643 nvram rw nvram:
- - opaque w0 syslog:
- - network rw rcp:
- - network rw http:
- - network rw ftp:
- - network rw scp:
- - network rw https:
- - opaque ro cnss:
- - opaque rw revrcsf:
```

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
### Table 108: show file systems Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size(b)</td>
<td>Amount of memory in the file system in bytes.</td>
</tr>
<tr>
<td>Free(b)</td>
<td>Amount of free memory in the file system in bytes.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of file system.</td>
</tr>
<tr>
<td></td>
<td>disk—The file system is for a flash memory device, USB flash, and</td>
</tr>
<tr>
<td></td>
<td>crashinfo file.</td>
</tr>
<tr>
<td></td>
<td>network—The file system for network devices; for example, an FTP server</td>
</tr>
<tr>
<td></td>
<td>or and HTTP server.</td>
</tr>
<tr>
<td></td>
<td>nvrarn—The file system is for a NVRAM device.</td>
</tr>
<tr>
<td></td>
<td>opaque—The file system is a locally generated pseudo file system</td>
</tr>
<tr>
<td></td>
<td>(for example, the system) or a download interface, such as brimux.</td>
</tr>
<tr>
<td></td>
<td>unknown—The file system is an unknown type.</td>
</tr>
<tr>
<td>Flags</td>
<td>Permission for file system.</td>
</tr>
<tr>
<td></td>
<td>ro—read-only.</td>
</tr>
<tr>
<td></td>
<td>rw—read/write.</td>
</tr>
<tr>
<td></td>
<td>wo—write-only.</td>
</tr>
</tbody>
</table>
### Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the `cd filesystem` privileged EXEC command. You can set the default file system to omit the `filesystem:` argument from related commands. For example, for all privileged EXEC commands that have the optional `filesystem:` argument, the system uses the file system specified by the `cd` command.

By default, the default file system is `flash:`.

You can display the current default file system as specified by the `cd` command by using the `pwd` privileged EXEC command.

### Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command. To display information about files on a file system, use one of the privileged EXEC commands listed in the following table.
### Changing Directories and Displaying the Working Directory

Follow these steps to change directories and to display the working directory:

#### SUMMARY STEPS

1. `enable`
2. `dir filesystem:`
3. `cd directory_name`
4. `pwd`
5. `cd`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dir filesystem:</td>
<td>Displays the directories on the specified file system.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>For <code>filesystem</code>, use flash: for the system board flash device.</td>
</tr>
<tr>
<td>Switch# dir flash:</td>
<td></td>
<td>To access flash partitions of switch members in a stack, use flash-n where n is the stack member number. For example, flash-4.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cd directory_name</td>
<td>Navigates to the specified directory.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>The command example shows how to navigate to the directory named <code>new_configs</code>.</td>
</tr>
<tr>
<td>Switch# cd new_configs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating Directories

Beginning in privileged EXEC mode, follow these steps to create a directory:

**SUMMARY STEPS**

1. `dir filesystem:
2. mkdir directory_name
3. dir filesystem:

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>dir filesystem:</code></td>
<td>Displays the directories on the specified file system. For <code>filesystem:</code> use flash: for the system board flash device.</td>
</tr>
<tr>
<td>Switch# <code>dir flash:</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>mkdir directory_name</code></td>
<td>Creates a new directory. Directory names are case sensitive and are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, slashes, quotes, semicolons, or colons.</td>
</tr>
<tr>
<td>Switch# <code>mkdir new_configs</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>dir filesystem:</code></td>
<td>Verifies your entry.</td>
</tr>
<tr>
<td>Switch# <code>dir flash:</code></td>
<td></td>
</tr>
</tbody>
</table>

Removing Directories

To remove a directory with all its files and subdirectories, use the `delete /force /recursive filesystem:/file-url` privileged EXEC command.
Use the `/recursive` keyword to delete the named directory and all subdirectories and the files contained in it. Use the `/force` keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process.

For `filesystem`, use `flash` for the system board flash device. For `file-url`, enter the name of the directory to be deleted. All of the files in the directory and the directory are removed.

⚠️ Caution
When directories are deleted, their contents cannot be recovered.

### Copying Files

To copy a file from a source to a destination, use the `copy source-url destination-url` privileged EXEC command. For the source and destination URLs, you can use `running-config` and `startup-config` keyword shortcuts. For example, the `copy running-config startup-config` command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special filesystems (`xmodem:`, `ymodem:`) as the source for the file from a network machine that uses the Xmodem or Ymodem protocol.

Network file system URLs include `ftp:`, `rcp:`, and `tftp:` and have these syntaxes:

- FTP—ftp://[username [:password]@location]/directory]/filename
- RCP—rcp://[username@location]/directory]/filename
- TFTP—tftp://[location]/directory]/filename

Local writable file systems include `flash:`.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the `copy flash: flash:` command is invalid)

### Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the `delete [/force] [/recursive] [filesystem:]file-url` privileged EXEC command.

Use the `/recursive` keyword for deleting a directory and all subdirectories and the files contained in it. Use the `/force` keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the `/force` and `/recursive` keywords for deleting old software images that were installed by using the `archive download-sw` command but are no longer needed.

If you omit the `filesystem` option, the switch uses the default device specified by the `cd` command. For `file-url`, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.
Caution

When files are deleted, their contents cannot be recovered.

This example shows how to delete the file myconfig from the default flash memory device:

Switch# delete myconfig

Creating, Displaying and Extracting Files

You can create a file and write files into it, list the files in a file, and extract the files from a file as described in the next sections.

Beginning in privileged EXEC mode, follow these steps to create a file, display the contents, and extract it:

SUMMARY STEPS

1. archive tar /create destination-url flash:/file-url
2. archive tar /table source-url
3. archive tar /xtract source-url flash:/file-url [dir/file...]
4. more [/ascii | /binary | /ebcdic] /file-url

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> archive tar /create destination-url flash:/file-url <strong>Example:</strong></td>
<td>Creates a file and adds files to it.</td>
</tr>
<tr>
<td>switch# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs</td>
<td>For destination-url, specify the destination URL alias for the local or network file system and the name of the file to create:</td>
</tr>
<tr>
<td></td>
<td>• Local flash file system syntax:</td>
</tr>
<tr>
<td></td>
<td>• FTP syntax:</td>
</tr>
<tr>
<td></td>
<td>• RCP syntax:</td>
</tr>
<tr>
<td></td>
<td>• TFTP syntax:</td>
</tr>
<tr>
<td></td>
<td>• flash:</td>
</tr>
<tr>
<td></td>
<td>• ftp:[//username[:password]@[location]/directory/-filename.</td>
</tr>
<tr>
<td></td>
<td>• rcp:[//username@location]/directory/-filename.</td>
</tr>
<tr>
<td></td>
<td>• tftp:[//location]/directory/-filename.</td>
</tr>
<tr>
<td></td>
<td>For flash:/file-url, specify the location on the local flash file system in which the new file is created. You can also specify an optional list of files or directories within the source directory to add to the new file. If none are specified, all files and directories at this level are written to the newly created file.</td>
</tr>
</tbody>
</table>

<p>| <strong>Step 2</strong> archive tar /table source-url <strong>Example:</strong> | Displays the contents of a file. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `switch# archive tar /table flash: /new_configs` | For source-url, specify the source URL alias for the local or network file system. The `-filename` is the file to display. These options are supported:  
  - Local flash file system syntax:  
    `flash:`  
  - FTP syntax:  
    `ftp://[username:password@]location/directory/-filename`.  
  - RCP syntax:  
    `rcp://username@location/directory/-filename`.  
  - TFTP syntax:  
    `tftp://[location]/directory/-filename`.  
  You can also limit the file displays by specifying a list of files or directories after the file. Only those files appear. If none are specified, all files and directories appear. |
| **Step 3** `archive tar /xtract source-url flash:file-url [dir/file...]` | Extracts a file into a directory on the flash file system.  
For source-url, specify the source URL alias for the local file system. The `-filename` is the file from which to extract files. These options are supported:  
  - Local flash file system syntax:  
    `flash:`  
  - FTP syntax:  
    `ftp://[username:password@]location/directory/-filename`.  
  - RCP syntax:  
    `rcp://username@location/directory/-filename`.  
  - TFTP syntax:  
    `tftp://[location]/directory/-filename`.  
For flash:file-url [dir/file...], specify the location on the local flash file system from which the file is extracted. Use the dir/file... option to specify a list of files or directories within the file to be extracted. If none are specified, all files and directories are extracted. |
| **Step 4** `more [ /ascii | /binary | /ebcdic] /file-url` | Displays the contents of any readable file, including a file on a remote file system.  
Example:  
`switch# more  
flash:/new-configs` |
Working with Configuration Files

Information on Configuration Files

Configuration files contain commands entered to customize the function of the Cisco IOS software. A way to create a basic configuration file is to use the setup program or to enter the setup privileged EXEC command.

You can copy (download) configuration files from a TFTP, FTP, or RCP server to the running configuration or startup configuration of the switch. You might want to perform this for one of these reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another switch. For example, you might add another switch to your network and want it to have a configuration similar to the original switch. By copying the file to the new switch, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on all the switches in your network so that all the switches have similar configurations.

You can copy (upload) configuration files from the switch to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your switch configuration. Configuration files can contain some or all of the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- We recommend that you connect through the console port or Ethernet management port for the initial configuration of the switch. If you are accessing the switch through a network connection instead of through a direct connection to the console port or Ethernet management port, keep in mind that some configuration changes (such as changing the switch IP address or disabling ports) can cause a loss of connectivity to the switch.

- If no password has been set on the switch, we recommend that you set one by using the `enable secret` `secret-password` global configuration command.
The `copy { ftp: | rcp: | tftp: } system:running-config` privileged EXEC command loads the configuration files on the switch as if you were entering the commands at the command line. The switch does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the `copy { ftp: | rcp: | tftp: } nvram:startup-config` privileged EXEC command), and reload the switch.

---

**Configuration File Types and Location**

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the `copy running-config startup-config` privileged EXEC command.

The running configuration is saved in DRAM; the startup configuration is stored in the NVRAM section of flash memory.

**Creating a Configuration File By Using a Text Editor**

When creating a configuration file, you must list commands logically so that the system can respond appropriately. This is one method of creating a configuration file:

**SUMMARY STEPS**

1.  
2.  
3.  
4.  
5.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Copy an existing configuration from a switch to a server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Extract the portion of the configuration file with the desired commands, and save it in a new file.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Make sure the permissions on the file are set to world-read.</td>
</tr>
</tbody>
</table>

### Copying Configuration Files By Using TFTP

You can configure the switch by using configuration files you create, download from another switch, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage.

### Preparing to Download or Upload a Configuration File By Using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the `/etc/inetd.conf` file contains this line:

  ```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the `/etc/services` file contains this line:

  ```
tftp 69/udp
  ```

- **Note**: You must restart the `inetd` daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the `inetd` process and restart it, or enter a `fastboot` command (on the SunOS 4.x) or a `reboot` command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnet if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the `ping` command.

- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually /tftpboot on a UNIX workstation).

- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-readable.

- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the `touch filename` command, where `filename` is the name of the file you will use when uploading it to the server.

- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.
Downloading the Configuration File By Using TFTP

To configure the switch by using a configuration file downloaded from a TFTP server, follow these steps:

**SUMMARY STEPS**

1. 
2. 
3. 
4. 

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Copy the configuration file to the appropriate TFTP directory on the workstation.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Verify that the TFTP server is properly configured.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Log into the switch through the console port, the Ethernet management port, or a Telnet session.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Download the configuration file from the TFTP server to configure the switch. Specify the IP address or hostname of the TFTP server and the name of the file to download. Use one of these privileged EXEC commands: <code>copy tftp://[location]/directory/filename</code> <code>system:running-config</code> <code>copy tftp://[location]/directory/filename</code> <code>nvram:startup-config</code> <code>copy tftp://[location]/directory/filename</code> <code>flash[n]/directory/startup-config</code> <strong>Note</strong> You can only enter the <code>flash</code> parameter (for example, <code>flash3</code>) on Catalyst 3750-E switches. The configuration file downloads, and the commands are executed as the file is parsed line-by-line.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to configure the software from the file tokyo-config at IP address 172.16.2.155:

```
Switch# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```
Uploading the Configuration File By Using TFTP

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

SUMMARY STEPS

1. Verify that the TFTP server is properly configured.
2. Log into the switch through the console port, the Ethernet management port, or a Telnet session.
3. Upload the switch configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify that the TFTP server is properly configured.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port, the Ethernet management port, or a Telnet session.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Upload the switch configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename. Use one of these privileged EXEC commands:</td>
</tr>
<tr>
<td></td>
<td>• copy system:running-config tftp://[//location]/directory/[filename]</td>
</tr>
<tr>
<td></td>
<td>• copy nvram:startup-config tftp://[//location]/directory/[filename]</td>
</tr>
<tr>
<td></td>
<td>• copy flash[n]:/directory/startup-config tftp://[//location]/directory/[filename]</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You can only enter the flash parameter (for example, flash3) on Catalyst 3750-E switches. The file is uploaded to the TFTP server.</td>
</tr>
</tbody>
</table>

Example

This example shows how to upload a configuration file from a switch to a TFTP server:

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
# Writing tokyo-config!!! [OK]
```

Copying a Configuration File from the Switch to an FTP Server

You can copy a configuration file from the switch to an FTP server.
Understanding the FTP Username and Password

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the switch to a server using FTP, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The username specified in the `copy` EXEC command, if a username is specified.
2. The username set by the `ip ftp username` global configuration command, if the command is configured.
3. Anonymous.

The switch sends the first valid password it encounters in the following sequence:

1. The password specified in the `copy` command, if a password is specified.
2. The password set by the `ip ftp password` command, if the command is configured.
3. The switch forms a password `username @switchname.domain`. The variable `username` is the username associated with the current session, `switchname` is the configured host name, and `domain` is the domain of the switch.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the switch.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your FTP server for more information.

Use the `ip ftp username` and `ip ftp password` global configuration commands to specify a username and password for all copies. Include the username in the `copy` EXEC command if you want to specify a username for that copy operation only.

Preparing to Download or Upload a Configuration File By Using FTP

Before you begin downloading or uploading a configuration file by using FTP, do these tasks:

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the `ping` command.

- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the `show users` privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the `ip ftp username username` global configuration command during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the `copy` command if you want to specify a username for only that copy operation.

- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.


## Downloading a Configuration File By Using FTP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

### SUMMARY STEPS

1. configure terminal
2. ip ftp username \( \text{username} \)
3. ip ftp password \( \text{password} \)
4. end
5. Do one of the following:
   - copy system:running-config ftp: [[//[username :password @]location]/directory ]/filename ]
   - copy nvram:startup-config ftp: [[//[username :password @]location]/directory ]/filename ]

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** configure terminal | Enter global configuration mode on the switch.  
This step is required only if you override the default remote username or password (see Steps 2, 3, and 4). |
| **Step 2** ip ftp username \( \text{username} \) | (Optional) Change the default remote username. |
| **Step 3** ip ftp password \( \text{password} \) | (Optional) Change the default password. |
| **Step 4** end | Return to privileged EXEC mode. |
| **Step 5** Do one of the following:  
   - copy system:running-config ftp: [ [ [// [ username :password @ ] location ]/directory ]/filename ]  
   - copy nvram:startup-config ftp: [ [ [// [ username :password @ ] location ]/directory ]/filename ] | Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file. |

### Example

This example shows how to copy a configuration file named host1-config from the netadmin1 directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config  
```

Configure using host1-config from 172.16.101.101? [confirm]  
Connected to 172.16.101.101  
Loading 1112 byte file host1-config:![OK]

Switch#  
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101

This example shows how to specify a remote username of netadmin1. The software copies the configuration file host2-config from the netadmin1 directory on the remote server with an IP address of 172.16.101.101 to the switch startup configuration.
Uploading a Configuration File By Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

SUMMARY STEPS

1. configure terminal
2. ip ftp username username
3. ip ftp password password
4. end
5. Do one of the following:
   - copy system:running-config ftp: [///[username [password ]@[location]/directory ]/filename ] or
   - copy nvram:startup-config ftp: [///[username [password ]@[location]/directory ]/filename ]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode on the switch.</td>
</tr>
<tr>
<td>Step 1: configure terminal</td>
<td>This step is required only if you override the default remote</td>
</tr>
<tr>
<td></td>
<td>username or password (see Steps 2, 3, and 4).</td>
</tr>
<tr>
<td>Step 2: ip ftp username username</td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 3: ip ftp password password</td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5: Do one of the following:</td>
<td>Using FTP, store the switch running or startup configuration</td>
</tr>
<tr>
<td></td>
<td>file to the specified location.</td>
</tr>
</tbody>
</table>
Example

This example shows how to copy the running configuration file named switch2-config to the netadmin1 directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config
ftp://netadmin1:mypass@172.16.101.101/switch2-config
Write file switch2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Switch#
```

This example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101?[confirm]
!OK
```

Copying Configuration Files By Using RCP

The RCP provides another method of downloading, uploading, and copying configuration files between remote hosts and the switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the switch to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the `copy` command if a username is specified.
- The username set by the `ip rcmd remote-username username` global configuration command if the command is configured.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the `username` command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated...
with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

**Preparation to Download or Upload a Configuration File By Using RCP**

Before you begin downloading or uploading a configuration file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the `ping` command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the show users privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the `ip rcmd remote-username` global configuration command to be used during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the copy command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it must be properly configured to accept the RCP write request from the user on the switch. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose that the switch contains these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch IP address translates to Switch1.company.com, the .rhosts file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

**Downloading a Configuration File By Using RCP**

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

**SUMMARY STEPS**

1. configure terminal
2. ip rcmd remote-username `username`
3. end
4. Do one of the following:
   - `copy rcp:[//[username@]location]/directory]/filename/system:running-config`
   - `copy rcp:[//[username@]location]/directory]/filename/nvram:startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode on the switch.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>This step is required only if you override the default remote username (see Steps 2 and 3).</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 2

*ip rcmd remote-username username*

(Optional) Change the default remote username.

#### Step 3

*end*

Return to privileged EXEC mode.

#### Step 4

Do one of the following:

- **copy**
  
  `rcp://username@location/directory/filename/system:running-config`

- **copy**
  
  `rcp://username@location/directory/filename/nvram:startup-config`

Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

### Example

This example shows how to copy a configuration file named host1-config from the netadmin1 directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the switch:

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of netadmin1. Then it copies the configuration file host2-config from the netadmin1 directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp://netadmin1@172.16.101.101/host2-config nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV: Non-volatile store configured from host2-config by rcp from 172.16.101.101
```

### Uploading a Configuration File By Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP

**SUMMARY STEPS**

1. configure terminal
2. *ip rcmd remote-username username*
3. end
4. Do one of the following:
   • `copy system:running-config rcp://[username@location]/directory/[filename]`
   • `copy nvram:startup-config rcp://[username@location]/directory/[filename]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode on the switch. This step is required only if you override the default remote username (see Steps 2 and 3).</td>
</tr>
<tr>
<td><strong>Step 2</strong> ip rcmd remote-username <em>username</em></td>
<td>(Optional) Specify the remote username.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Do one of the following:</td>
<td>Using RCP, copy the configuration file from a switch running configuration or startup configuration file to a network server.</td>
</tr>
<tr>
<td>• <code>copy system:running-config rcp://[username@location]/directory/[filename]</code></td>
<td></td>
</tr>
<tr>
<td>• <code>copy nvram:startup-config rcp://[username@location]/directory/[filename]</code></td>
<td></td>
</tr>
</tbody>
</table>

**Example**

This example shows how to copy the running configuration file named switch2-config to the netadmin1 directory on the remote host with an IP address of 172.16.101.101:

```bash
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-config
```

This example shows how to store a startup configuration file on a server:

```bash
Switch# copy nvram:startup-config rcp://[username@location]/directory/[filename] rcp://172.16.101.101
```

**Clearing Configuration Information**

You can clear the configuration information from the startup configuration. If you reboot the switch with no startup configuration, the switch enters the setup program so that you can reconfigure the switch with all new settings.
Clearing the Startup Configuration File

To clear the contents of your startup configuration, use the `erase nvram` or the `erase startup-config` privileged EXEC command.

**Note**
You cannot restore the startup configuration file after it has been deleted.

Deleting a Stored Configuration File

To delete a saved configuration from flash memory, use the `delete flash:filename` privileged EXEC command. Depending on the setting of the file prompt global configuration command, you might be prompted for confirmation before you delete a file. By default, the switch prompts for confirmation on destructive file operations. For more information about the file prompt command, see the Cisco IOS Command Reference for Release 12.4.

**Note**
You cannot restore a file after it has been deleted.

Replacing and Rolling Back Configurations

The configuration replacement and rollback feature replaces the running configuration with any saved Cisco IOS configuration file. You can use the rollback function to roll back to a previous configuration.

Information on Configuration Replacement and Rollback

**Configuration Archive**

The Cisco IOS configuration archive is intended to provide a mechanism to store, organize, and manage an archive of Cisco IOS configuration files to enhance the configuration rollback capability provided by the `configure replace` command. Before this feature was introduced, you could save copies of the running configuration using the `copy running-config destination-url` command, storing the replacement file either locally or remotely. However, this method lacked any automated file management. On the other hand, the Configuration Replace and Configuration Rollback feature provides the capability to automatically save copies of the running configuration to the Cisco IOS configuration archive. These archived files serve as checkpoint configuration references and can be used by the `configure replace` command to revert to previous configuration states.

The `archive config` command allows you to save Cisco IOS configurations in the configuration archive using a standard location and filename prefix that is automatically appended with an incremental version number (and optional timestamp) as each consecutive file is saved. This functionality provides a means for consistent identification of saved Cisco IOS configuration files. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved in the archive, the oldest file is automatically deleted when the next, most recent file is saved. The `show archive` command displays information for all configuration files saved in the Cisco IOS configuration archive.
The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the `configure replace` command, can be located on the following file systems: FTP, HTTP, RCP, TFTP.

**Configuration Replace**

The `configure replace` privileged EXEC command replaces the running configuration with any saved configuration file. When you enter the `configure replace` command, the running configuration is compared with the specified replacement configuration, and a set of configuration differences is generated. The resulting differences are used to replace the configuration. The configuration replacement operation is usually completed in no more than three passes. To prevent looping behavior no more than five passes are performed.

You can use the `copy source-url running-config` privileged EXEC command to copy a stored configuration file to the running configuration. When using this command as an alternative to the `configure replace target-url` privileged EXEC command, note these major differences:

- The `copy source-url running-config` command is a merge operation and preserves all the commands from both the source file and the running configuration. This command does not remove commands from the running configuration that are not present in the source file. In contrast, the `configure replace target-url` command removes commands from the running configuration that are not present in the replacement file and adds commands to the running configuration that are not present.

- You can use a partial configuration file as the source file for the `copy source-url running-config` command. You must use a complete configuration file as the replacement file for the `configure replace target-url` command.

**Configuration Rollback**

You can also use the `configure replace` command to roll back changes that were made since the previous configuration was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the configuration rollback capability reverts to a specific configuration based on a saved configuration file.

If you want the configuration rollback capability, you must first save the running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes by using the `configure replace target-url` command.

You can specify any saved configuration file as the rollback configuration. You are not limited to a fixed number of rollbacks, as is the case in some rollback models.

**Configuration Guidelines**

Follow these guidelines when configuring and performing configuration replacement and rollback:

- Make sure that the switch has free memory larger than the combined size of the two configuration files (the running configuration and the saved replacement configuration). Otherwise, the configuration replacement operation fails.

- Make sure that the switch also has sufficient free memory to execute the configuration replacement or rollback configuration commands.

- Certain configuration commands, such as those pertaining to physical components of a networking device (for example, physical interfaces), cannot be added or removed from the running configuration.

  - A configuration replacement operation cannot remove the `interface interface-id` command line from the running configuration if that interface is physically present on the device.
  
  - The `interface interface-id` command line cannot be added to the running configuration if no such interface is physically present on the device.
• When using the `configure replace` command, you must specify a saved configuration as the replacement configuration file for the running configuration. The replacement file must be a complete configuration generated by a Cisco IOS device (for example, a configuration generated by the `copy running-config` destination-url command).

**Note**

If you generate the replacement configuration file externally, it must comply with the format of files generated by Cisco IOS devices.

### Configuring the Configuration Archive

Using the `configure replace` command with the configuration archive and with the `archive config` command is optional but offers significant benefit for configuration rollback scenarios. Before using the `archive config command`, you must first configure the configuration archive. Starting in privileged EXEC mode, follow these steps to configure the configuration archive:

#### SUMMARY STEPS

1. `configure terminal`
2. `archive`
3. `path url`
4. `maximum number`
5. `time-period minutes`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> archive</td>
<td>Enter archive configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>path url</code></td>
<td>Specify the location and filename prefix for the files in the configuration archive.</td>
</tr>
</tbody>
</table>
| **Step 4** `maximum number` | *(Optional)* Set the maximum number of archive files of the running configuration to be saved in the configuration archive.

`number`—Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10.

**Note**

Before using this command, you must first enter the `path archive configuration command to specify the location and filename prefix for the files in the configuration archive.
Performing a Configuration Replacement or Rollback Operation

Starting in privileged EXEC mode, follow these steps to replace the running configuration file with a saved configuration file:

**SUMMARY STEPS**

1. `archive config`
2. `configure terminal`
3. `exit`
4. `configure replace target-url [list] [force] [time seconds] [nolock]`
5. `configure confirm`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 archive config | (Optional) Save the running configuration file to the configuration archive.  
**Note** Enter the `path` archive configuration command before using this command. |
| Step 2 configure terminal | Enter global configuration mode. |
| Step 3 exit | Make necessary changes to the running configuration |
| Step 4 exit | Return to privileged EXEC mode. |
| Step 5 configure replace target-url [list] [force] [time seconds] [nolock] | Replace the running configuration file with a saved configuration file.  
`target-url`—URL (accessible by the file system) of the saved configuration file that is to replace the running configuration, such as the configuration file created in Step 2 by using the `archive config` privileged EXEC command |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>list — Display a list of the command entries applied by the software parser during each pass of the configuration replacement operation. The total number of passes also appears.</td>
<td></td>
</tr>
<tr>
<td>force — Replace the running configuration file with the specified saved configuration file without prompting you for confirmation.</td>
<td></td>
</tr>
<tr>
<td>timespecs — Specify the time (in seconds) within which you must enter the configure confirm command to confirm replacement of the running configuration file. If you do not enter the configure confirm command within the specified time limit, the configuration replacement operation is automatically stopped. (In other words, the running configuration file is restored to the configuration that existed before you entered the configure replace command).</td>
<td></td>
</tr>
<tr>
<td>You must first enable the configuration archive before you can use the time seconds command line option.</td>
<td></td>
</tr>
<tr>
<td>nolock — Disable the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replacement operation.</td>
<td></td>
</tr>
<tr>
<td>configure confirm — (Optional) Confirm replacement of the running configuration with a saved configuration file.</td>
<td></td>
</tr>
<tr>
<td>Use this command only if the time seconds keyword and argument of the configure replace command are specified.</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config — (Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

## Working with Software Images

### Information on Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, the Cisco IOS code, and the embedded device manager software.

- **Note**
  Instead of using the copy privileged EXEC command or the archive tar privileged EXEC command, we recommend using the archive download-sw and archive upload-sw privileged EXEC commands to download and upload software image files.

---

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)

1046
You can download a switch image file from a TFTP, FTP, or RCP server to upgrade the switch software. If you do not have access to a TFTP server, you can download a software image file directly to your PC or workstation by using a web browser (HTTP) and then by using the device manager or Cisco Network Assistant to upgrade your switch. For information about upgrading your switch by using a TFTP server or a web browser (HTTP), see the release notes.

You can replace the current image with the new one or keep the current image in flash memory after a download.

You upload a switch image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same switch or to another of the same type.

The protocol that you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

Note

For a list of software images and the supported upgrade paths, see the release notes.

Image Location on the Switch

The Cisco IOS image is stored as a .bin file in a directory that shows the version number. A subdirectory contains the files needed for web management. The image is stored on the system board flash memory (flash:).

You can use the show version privileged EXEC command to see the software version that is currently running on your switch. In the display, check the line that begins with System image file is.... It shows the directory name in flash memory where the image is stored.

You can also use the dir filesystem: privileged EXEC command to see the directory names of other software images that might be stored in flash memory.

File Format of Images on a Server or Cisco.com

Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- An info file, which serves as a table of contents for the tar file
- One or more subdirectories containing other images and files, such as Cisco IOS images and web management files

This example shows some of the information contained in the info file. The table provides additional details about this information:

```
system_type:0x00000000:image-name
image_family:xxxx
stacking_number:x
info_end:

version_suffix:xxxx
version_directory:image-name
image_system_type_id:0x00000000
image_name:image-nameB.bin
ios_image_file_size:6398464
total_image_file_size:8133632
```
Table 110: info File Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version_suffix</td>
<td>Specifies the Cisco IOS image version string suffix</td>
</tr>
<tr>
<td>version_directory</td>
<td>Specifies the directory where the Cisco IOS image and the HTML subdirectory are installed</td>
</tr>
<tr>
<td>image_name</td>
<td>Specifies the name of the Cisco IOS image within the tar file</td>
</tr>
<tr>
<td>ios_image_file_size</td>
<td>Specifies the Cisco IOS image size in the tar file, which is an approximate measure of how much flash memory is required to hold just the Cisco IOS image</td>
</tr>
<tr>
<td>total_image_file_size</td>
<td>Specifies the size of all the images (the Cisco IOS image and the web management files) in the tar file, which is an approximate measure of how much flash memory is required to hold them</td>
</tr>
<tr>
<td>image_feature</td>
<td>Describes the core functionality of the image</td>
</tr>
<tr>
<td>image_min_dram</td>
<td>Specifies the minimum amount of DRAM needed to run this image</td>
</tr>
<tr>
<td>image_family</td>
<td>Describes the family of products on which the software can be installed</td>
</tr>
</tbody>
</table>

Copying Image Files Using TFTP

You can download a switch image from a TFTP server or upload the image from the switch to a TFTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another switch of the same type.

Note

Instead of using the `copy` privileged EXEC command or the `archive tar` privileged EXEC command, we recommend using the `archive download-sw` and `archive upload-sw` privileged EXEC commands to download and upload software image files.
Preparing to Download or Upload an Image File By Using TFTP

Before you begin downloading or uploading an image file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot

  Make sure that the /etc/services file contains this line:

  tftp 69/udp

  You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a fastboot command (on the SunOS 4.x) or a reboot command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the ping command.

- Ensure that the image to be downloaded is in the correct directory on the TFTP server (usually /tftpboot on a UNIX workstation).

- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.

- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the touch filename command, where filename is the name of the file you will use when uploading the image to the server.

- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading an Image File By Using TFTP

You can download a new image file and replace the current image or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image. To keep the current image, go to Step 3.

SUMMARY STEPS

1.
2.
3. archive download-sw/overwrite/reload tftp: [ [ //location] /directory]/image-name.tar
4. archive download-sw/leave-old-sw/reload tftp: [ [ //location] /directory]/image-name.tar
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
<td>Copy the image to the appropriate TFTP directory on the workstation. Make sure that the TFTP server is properly configured.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>archive download-sw/overwrite/reload</code></td>
<td>Download the image file from the TFTP server to the switch, and overwrite the current image.</td>
</tr>
<tr>
<td></td>
<td><code>tftp: [ [ //location ] /directory ] /image-name.tar</code></td>
<td>- The <code>overwrite</code> option overwrites the software image in flash memory with the downloaded image.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The <code>reload</code> option reloads the system after downloading the image unless the configuration has been changed and not been saved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For <code>//location</code>, specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For <code>/directory/image-name.tar</code> specify the directory (optional) and the image to download. Directory and image names are case sensitive.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>archive download-sw/leave-old-sw/reload</code></td>
<td>Download the image file from the TFTP server to the switch, and keep the current image.</td>
</tr>
<tr>
<td></td>
<td><code>tftp: [ [ //location ] /directory ] /image-name.tar</code></td>
<td>- The <code>leave-old-sw</code> option keeps the old software version after a download.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The <code>reload</code> option reloads the system after downloading the image unless the configuration has been changed and not been saved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For <code>//location</code>, specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For <code>/directory/image-name.tar</code> specify the directory (optional) and the image to download. Directory and image names are case sensitive.</td>
</tr>
</tbody>
</table>

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the `overwrite` option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note** If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the `overwrite` option.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you specify the /leave-old-sw, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed. The algorithm installs the downloaded image on the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image. If you keep the old image during the download process (you specified the /leave-old-sw keyword), you can remove it by entering the delete/force/recursive filesystem :/file-url privileged EXEC command. For filesystem, use flash: for the system board flash device. For file-url, enter the directory name of the old image. All the files in the directory and the directory are removed. <strong>Note</strong> For the download and upload algorithms to operate properly, do not rename image names.</td>
<td></td>
</tr>
</tbody>
</table>

### Uploading an Image File Using TFTP

You can upload an image from the switch to a TFTP server. You can later download this image to the switch or to another switch of the same type.

Use the upload feature only if the web management pages associated with the embedded device manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to a TFTP server:

**SUMMARY STEPS**
1. 
2. 
3. **archive upload-sw tftp:**[// location ]/directory ]/image-name .tar

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Make sure the TFTP server is properly configured</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
</tbody>
</table>
| Step 3 **archive upload-sw tftp:**[// location ]/directory ]/image-name .tar | Upload the currently running switch image to the TFTP server.  
  • For // location , specify the IP address of the TFTP server. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For /directory/image-name.tar</td>
<td>specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <code>image-name.tar</code> is the name of the software image to be stored on the server.</td>
</tr>
<tr>
<td>The <code>archive upload-sw</code> privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>For the download and upload algorithms to operate properly, do not rename image names.</td>
</tr>
</tbody>
</table>

### Copying Image Files Using FTP

You can download a switch image from an FTP server or upload the image from the switch to an FTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the switch or another switch of the same type.

**Note**

Instead of using the `copy` privileged EXEC command or the `archive tar` privileged EXEC command, we recommend using the `archive download-sw` and `archive upload-sw` privileged EXEC commands to download and upload software image files.

### Preparing to Download or Upload an Image File By Using FTP

You can copy image files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the switch to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the `archive download-sw` or `archive upload-sw` privileged EXEC command if a username is specified.
- The username set by the `ip ftp username` username global configuration command if the command is configured.
- Anonymous.

The switch sends the first valid password in this list:
• The password specified in the `archive download-sw` or `archive upload-sw` privileged EXEC command if a password is specified.

• The password set by the `ip ftp password` password global configuration command if the command is configured.

• The switch forms a password named `username@switchname.domain`. The variable `username` is the username associated with the current session, `switchname` is the configured hostname, and `domain` is the domain of the switch.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

Use the `ip ftp username` and `ip ftp password` commands to specify a username and password for all copies. Include the username in the `archive download-sw` or `archive upload-sw` privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, do these tasks:

• Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the `ping` command.

• If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the `show users` privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the `ip ftp username` username global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the `archive download-sw` or `archive upload-sw` privileged EXEC command if you want to specify a username for that operation only.

• When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

**Downloading an Image File By Using FTP**

You can download a new image file and overwrite the current image or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 7 to download a new image from an FTP server and overwrite the existing image. To keep the current image, go to Step 7.

**SUMMARY STEPS**

1. 
2. 
3. `configure terminal`
4. `ip ftp username username`
5. `ip ftp password password`
## Downloading an Image File By Using FTP

6. end
7. `archive download-sw /overwrite/reload
   ftp: [ [ //username [:password] @location ] /directory ] /image-name.tar`
8. `archive download-sw /leave-old-sw/reload
   ftp: [ [ //username [:password] @location ] /directory ] /image-name.tar`

<table>
<thead>
<tr>
<th>DETAILED STEPS</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
<td>Verify that the FTP server is properly configured.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ip ftp username username</code></td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ip ftp password password</code></td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| Step 7         | `archive download-sw /overwrite/reload
   ftp: [ [ //username [:password] @location ] /directory ] /image-name.tar` | Download the image file from the FTP server to the switch, and overwrite the current image. |
|                |                   | • The /overwrite option overwrites the software image in flash memory with the downloaded image. |
|                |                   | • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. |
|                |                   | • For //username [:password]specify the username and password; these must be associated with an account on the FTP server. |
|                |                   | • For @ location, specify the IP address of the FTP server. |
|                |                   | • For directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive. |
| Step 8         | `archive download-sw /leave-old-sw/reload
   ftp: [ [ //username [:password] @location ] /directory ] /image-name.tar` | Download the image file from the FTP server to the switch, and keep the current image. |
<p>|                |                   | • The /leave-old-sw option keeps the old software version after a download. |
|                |                   | • The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved. |
|                |                   | • For //username [:password]specify the username and password; these must be associated with an account on the FTP server. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For @ location, specify the IP address of the FTP server.</td>
<td></td>
</tr>
<tr>
<td>• For directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive.</td>
<td></td>
</tr>
</tbody>
</table>

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the /overwrite option, the download algorithm removes the existing image on the flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note** If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the /overwrite option.

If you specify the /leave-old-sw, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the /leave-old-sw keyword), you can remove it by entering the delete force recursive filesystem:/file-url privileged EXEC command. For filesystem, use flash: for the system board flash device. For file-url, enter the directory name of the old software image. All the files in the directory and the directory are removed.

**Note** For the download and upload algorithms to operate properly, do not rename image names.

---

**Uploading an Image File By Using FTP**

You can upload an image from the switch to an FTP server. You can later download this image to the same switch or to another switch of the same type.

Use the upload feature only if the web management pages associated with the embedded device manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:
### SUMMARY STEPS

1. **configure terminal**
2. **ip ftp username** `username`
3. **ip ftp password** `password`
4. **end**
5. **archive upload-sw ftp:** `[[ // [username[:password]@location]/directory]/image-name.tar`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>ip ftp username</strong> <code>username</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ip ftp password</strong> <code>password</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>archive upload-sw ftp:</strong> <code>[[ // [username[:password]@location]/directory]/image-name.tar</code></td>
</tr>
</tbody>
</table>

- For `//username:password`, specify the username and password. These must be associated with an account on the FTP server.
- For `@location`, specify the IP address of the FTP server.
- For `/directory/image-name.tar`, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The `image-name.tar` is the name of the software image to be stored on the server.

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.

**Note** For the download and upload algorithms to operate properly, do not rename image names.

---

### Copying Image Files Using RCP

You can download a switch image from an RCP server or upload the image from the switch to an RCP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download. You upload a switch image file to a server.
for backup purposes. You can use this uploaded image for future downloads to the same switch or another of the same type.

**Note**

Instead of using the `copy` privileged EXEC command or the `archive tar` privileged EXEC command, we recommend using the `archive download-sw` and `archive upload-sw` privileged EXEC commands to download and upload software image files.

---

**Preparing to Download or Upload an Image File Using RCP**

RCP provides another method of downloading and uploading image files between remote hosts and the switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the `rsh` server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (`rsh`). (Most UNIX systems support `rsh`.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the switch to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the `archive download-sw` or `archive upload-sw` privileged EXEC command if a username is specified.
- The username set by the `ip rcmd remote-username username` global configuration command if the command is entered.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the `username` command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the image file is written to or copied from the directory associated with the remote username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (`rsh`).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the `ping` command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the `show users` privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the `ip rcmd remote-username username` global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this
username is used, and there is no need to set the RCP username. Include the username in the archive download-sw or archive upload-sw privileged EXEC command if you want to specify a username only for that operation.

- When you upload an image to the RCP to the server, it must be properly configured to accept the RCP write request from the user on the switch. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server.

For example, suppose the switch contains these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch IP address translates to Switch1.company.com, the .rhosts file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

### Downloading an Image File using RCP

You can download a new image file and replace or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP server and overwrite the existing image. To keep the current image, go to Step 6.

**SUMMARY STEPS**

1. 
2. 
3. configure terminal
4. ip rcmd remote-username \textit{username}
5. end
6. archive download-sw \texttt{/overwrite/reload} 
   \texttt{rcp:[]://username@[location]/directory/image-name.tar}
7. archive download-sw \texttt{/leave-old-sw/reload} 
   \texttt{rcp:[]://username@[location]/directory/image-name.tar}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the RCP server is properly configured.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode. This step is required only if you</td>
</tr>
<tr>
<td></td>
<td>override the default remote username or password (see Steps 4, 5, and</td>
</tr>
<tr>
<td></td>
<td>6).</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rcmd remote-username \textit{username}</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the remote username.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Purpose

- **Command or Action**
  
  **Step 6**
  
  archive download-sw /overwrite/reload
  rcp://username@location/directory/image-name.tar

  Download the image file from the RCP server to the switch, and overwrite the current image.

  - The /overwrite option overwrites the software image in flash memory with the downloaded image.
  - The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved.
  - For //username specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username.
  - For @ location, specify the IP address of the RCP server.
  - For /directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

  **Step 7**
  
  archive download-sw /leave-old-sw/reload
  rcp://username@location/directory/image-name.tar

  Download the image file from the FTP server to the switch, and keep the current image.

  - The /leave-old-sw option keeps the old software version after a download.
  - The /reload option reloads the system after downloading the image unless the configuration has been changed and not been saved.
  - For //username specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username.
  - For @ location, specify the IP address of the RCP server.
  - For /directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

  The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the /overwrite option, the download algorithm removes the existing image on the flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.

  **Note** If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the /overwrite option.

  If you specify the /leave-old-sw, the existing files are not removed. If there is not enough space to install the new
Uploading an Image File using RCP

You can upload an image from the switch to an RCP server. You can later download this image to the same switch or to another switch of the same type.

The upload feature should be used only if the web management pages associated with the embedded device manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

**SUMMARY STEPS**

1. configure terminal
2. ip rcmd remote-username **username**
3. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 configure terminal   | Enter global configuration mode.  
<pre><code>                          | This step is required only if you override the default remote username or password (see Steps 2 and 3.) |
</code></pre>
<p>| Step 2 ip rcmd remote-username <strong>username</strong> | Optional) Specify the remote username. |
| Step 3 end                  | Return to privileged EXEC mode. |</p>
<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>archive upload-sw</td>
<td>Upload the currently running switch image to the RCP server.</td>
</tr>
<tr>
<td></td>
<td>rcp: [ [ [/ [username@] location] /directory] /image-name.tar</td>
<td>• For //username, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For @location, specify the IP address of the RCP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For /directory/image-name.tar, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The image-name.tar is the name of software image to be stored on the server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The archive upload-sw command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the tar file format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> For the download and upload algorithms to operate properly, do not rename image names.</td>
</tr>
</tbody>
</table>
Uploading an Image File using RCP
PART XII

VLAN

• Configuring VTP, on page 1065
• VLANs, on page 1087
• Configuring VLAN Trunks, on page 1105
• Configuring VMPS, on page 1125
• Configuring Voice VLANs, on page 1139
Chapter 54

Configuring VTP

• Finding Feature Information, on page 1065
• Prerequisites for VTP, on page 1065
• Restrictions for VTP, on page 1066
• Information About VTP, on page 1066
• How to Configure VTP, on page 1074
• Monitoring VTP, on page 1084
• Configuration Examples for VTP, on page 1084
• Where to Go Next, on page 1086
• Additional References, on page 1086
• Feature History and Information for VTP, on page 1086

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VTP

Before you create VLANs, you must decide whether to use the VLAN Trunking Protocol (VTP) in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.
The switch supports a total of 256 VLANs. If the switch is notified by VTP of a new VLAN and the switch is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the `show vlan` user EXEC command shows the VLAN in a suspended state.

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of another switch. Otherwise, the switch cannot receive any VTP advertisements.

### Restrictions for VTP

Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

The following are restrictions for configuring VTPs:

- It is normal to have approximately 10 access interfaces or 5 trunk interfaces to flap simultaneously with negligible impact to CPU utilization. If there are more interfaces that flap simultaneously, then CPU usage may be excessively high.

### Information About VTP

**VTP**

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

VTP version 1 and version 2 support only normal-range VLANs (VLAN IDs 1 to 1005). VTP version 3 supports the entire VLAN range (VLANs 1 to 4094). Extended range VLANs (VLANs 1006 to 4094) are supported only in VTP version 3.

You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured in the domain.

**VTP Domain**

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches or switch stacks under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

By default, the switch is in the VTP no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain.
name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch. However, configuration changes made when the switch is in this mode are saved in the switch running configuration and can be saved to the switch startup configuration file.

Related Topics
- Adding a VTP Client Switch to a VTP Domain, on page 1082
- Prerequisites for VTP

## VTP Modes

### Table 111: VTP Modes

<table>
<thead>
<tr>
<th>VTP Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP server</td>
<td>In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. VTP server is the default mode. In VTP server mode, VLAN configurations are saved in NVRAM. If the switch detects a failure while writing a configuration to NVRAM, VTP mode automatically changes from server mode to client mode. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.</td>
</tr>
</tbody>
</table>
VTP Mode | Description
--- | ---
VTP client | A VTP client functions like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode.

In VTP versions 1 and 2 in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode.

VTP transparent | VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode.

When the switch is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other switches. In this mode, VTP mode and domain name are saved in the switch running configuration, and you can save this information in the switch startup configuration file by using the `copy running-config startup-config` privileged EXEC command.

VTP off | A switch in VTP off mode functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks.

### Related Topics
- Prerequisites for VTP
- Configuring VTP Mode, on page 1074
- Example: Configuring Switch as VTP Server, on page 1085

### VTP Advertisements

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number
• Update identity and update timestamp
• MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN
• Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:
• VLAN IDs (including IEEE 802.1Q)
• VLAN name
• VLAN type
• VLAN state
• Additional VLAN configuration information specific to the VLAN type

In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

Related Topics
Prerequisites for VTP

VTP Version 2

If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

VTP version 2 supports these features that are not supported in version 1:
• Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs.
• Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the switch is operating in VTP server mode.
• Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Although VTP version 2 supports only one domain, a VTP version 2 transparent switch forwards a message only when the domain name matches.
• Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

Related Topics
Enabling the VTP Version , on page 1077

VTP Version 3

VTP version 3 supports these features that are not supported in version 1 or version 2:
• Enhanced authentication—You can configure the authentication as hidden or secret. When hidden, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the secret keyword, you can directly configure the password secret key.

• Support for extended range VLAN (VLANs 1006 to 4094) database propagation—VTP versions 1 and 2 propagate only VLANs 1 to 1005.

| Note | VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified. |

• Support for any database in a domain—In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.

• VTP primary server and VTP secondary servers—A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to its NVRAM.

By default, all devices come up as secondary servers. You can enter the vtp primary privileged EXEC command to specify a primary server. Primary server status is only needed for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers. Primary server status is lost if the device reloads or domain parameters change, even when a password is configured on the switch.

Related Topics
Enabling the VTP Version, on page 1077

VTP Pruning

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible switch trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported in all VTP versions.

With VTP versions 1 and 2, when you enable pruning on the VTP server, it is enabled for the entire VTP domain. In VTP version 3, you must manually enable pruning on each switch in the domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all switches in the VTP domain).

VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.
VTP Configuration Guidelines

VTP Configuration Requirements

When you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain.

VTP versions 1 and 2 do not support private VLANs. VTP version 3 does support private VLANs. If you configure private VLANs, the switch must be in VTP transparent mode. When private VLANs are configured on the switch, do not change the VTP mode from transparent to client or server mode.

VTP Settings

The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the switch running configuration file, and you can save it in the switch startup configuration file by entering the `copy running-config startup-config` privileged EXEC command. You must use this command if you want to save VTP mode as transparent, even if the switch resets.

When you save VTP information in the switch startup configuration file and reboot the switch, the switch configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

Domain Names for Configuring VTP

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

Note

If the NVRAM and DRAM storage is sufficient, all switches in a VTP domain should be in VTP server mode.

Caution

Do not configure a VTP domain if all switches are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Make sure that you configure at least one switch in the VTP domain for VTP server mode.
Passwords for the VTP Domain

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.

Caution

When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each switch in the domain.

Related Topics
- Configuring a VTP Version 3 Password, on page 1076
- Example: Configuring a Switch as the Primary Server, on page 1084

VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.

- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch (version 2 is disabled by default).

- If a switch running VTP version 1, but capable of running VTP version 2, receives VTP version 3 advertisements, it automatically moves to VTP version 2.

- If a switch running VTP version 3 is connected to a switch running VTP version 1, the VTP version 1 switch moves to VTP version 2, and the VTP version 3 switch sends scaled-down versions of the VTP packets so that the VTP version 2 switch can update its database.

- A switch running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.

- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it does not exchange VTP information with switches that have version 2 enabled.

- Cisco recommends placing VTP version 1 and 2 switches at the edge of the network because they do not forward VTP version 3 advertisements.

- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
• VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must configure these VLANs manually on each device. VTP version 3 supports extended-range VLANs and support for extended range VLAN database propagation.

• When a VTP version 3 device trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database on that particular trunk in VTP version 2 format. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.

• When a VTP version 3 device detects a VTP version 2 device on a trunk port, it continues to send VTP version 3 packets, in addition to VTP version 2 packets, to allow both kinds of neighbors to coexist on the same trunk.

• A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.

• Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or version 2 region.

• Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.

• VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device.

**Related Topics**

[Enabling the VTP Version](#), on page 1077

### Default VTP Configuration

The following table shows the default VTP configuration.

**Table 112: Default VTP Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP domain name</td>
<td>Null</td>
</tr>
<tr>
<td>VTP mode (VTP version 1 and version 2)</td>
<td>Server</td>
</tr>
<tr>
<td>VTP mode (VTP version 3)</td>
<td>The mode is the same as the mode in VTP version 1 or 2 before conversion to version 3.</td>
</tr>
<tr>
<td>VTP version</td>
<td>Version 1</td>
</tr>
<tr>
<td>MST database mode</td>
<td>Transparent</td>
</tr>
<tr>
<td>VTP version 3 server type</td>
<td>Secondary</td>
</tr>
<tr>
<td>VTP password</td>
<td>None</td>
</tr>
<tr>
<td>VTP pruning</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
How to Configure VTP

Configuring VTP Mode

You can configure VTP mode as one of these:

- **VTP server mode**—In VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.

- **VTP client mode**—In VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.

- **VTP transparent mode**—In VTP transparent mode, VTP is disabled on the switch. The switch does not send VTP updates and does not act on VTP updates received from other switch. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements on its trunk links.

- **VTP off mode**—VTP off mode is the same as VTP transparent mode except that VTP advertisements are not forwarded.

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vtp domain domain-name`
4. `vtp mode {client | server | transparent | off; {vlan | mst | unknown}}`
5. `vtp password password`
6. `end`
7. `show vtp status`
8. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3 | `vtp domain domain-name` | Configures the VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.  
This command is optional for modes other than server mode. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain.  
You should configure the VTP domain before configuring other VTP parameters. |
| Example: | `Switch(config)# vtp domain eng_group` |
| Step 4 | `vtp mode {client | server | transparent | off} {vlan | mst | unknown}` | Configures the switch for VTP mode (client, server, transparent, or off).  
- `vlan`—The VLAN database is the default if none are configured.  
- `mst`—The multiple spanning tree (MST) database.  
- `unknown`—An unknown database type. |
| Example: | `Switch(config)# vtp mode server` |
| Step 5 | `vtp password password` | (Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain. |
| Example: | `Switch(config)# vtp password mypassword` |
| Step 6 | `end` | Returns to privileged EXEC mode. |
| Example: | `Switch(config)# end` |
| Step 7 | `show vtp status` | Verifies your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display. |
| Example: | `Switch# show vtp status` |
| Step 8 | `copy running-config startup-config` | (Optional) Saves the configuration in the startup configuration file.  
Only VTP mode and domain name are saved in the switch running configuration and can be copied to the startup configuration file. |
| Example: | `Switch# copy running-config startup-config` |

### Related Topics

- [VTP Modes](#), on page 1067
Configuring a VTP Version 3 Password

You can configure a VTP version 3 password on the switch.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vtp password password [hidden | secret]`
4. `end`
5. `show vtp password`
6. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2**        | Enters global configuration mode. |
| `configure terminal` | |
| Example:           | |
| Switch# `configure terminal` | |

| **Step 3**        | (Optional) Sets the password for the VTP domain. The password can be 8 to 64 characters. |
| `vtp password password [hidden | secret]` | • (Optional) hidden—Saves the secret key generated from the password string in the nvram:vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password. |
| Example:           | • (Optional) secret—Directly configures the password. The secret password must contain 32 hexadecimal characters. |
| Switch(config)# `vtp password mypassword hidden` | |

| **Step 4**        | Returns to privileged EXEC mode. |
| `end`             | |
| Example:          | |
| Switch(config)# `end` | |

| **Step 5**        | Verifies your entries. The output appears like this: |
| `show vtp password` | |
### Configuring a VTP Version 3 Primary Server

When you configure a VTP server as a VTP primary server, the takeover operation starts.

**SUMMARY STEPS**

1. `vtp primary [vlan | mst] [force]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Changes the operational state of a switch from a secondary server (the default) to a primary server and advertises the configuration to the domain. If the switch password is configured as <em>hidden</em>, you are prompted to reenter the password.</td>
</tr>
<tr>
<td>`vtp primary [vlan</td>
<td>mst] [force]`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# vtp primary vlan force</code></td>
</tr>
<tr>
<td></td>
<td>• (Optional) <em>vlan</em>—Selects the VLAN database as the takeover feature. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <em>mst</em>—Selects the multiple spanning tree (MST) database as the takeover feature.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <em>force</em>—Overwrites the configuration of any conflicting servers. If you do not enter <em>force</em>, you are prompted for confirmation before the takeover.</td>
</tr>
</tbody>
</table>

**Related Topics**

- VTP Settings, on page 1071

---

### Enabling the VTP Version

VTP version 2 and version 3 are disabled by default.
• When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each switch.

• With VTP versions 1 and 2, you can configure the version only on switches in VTP server or transparent mode. If a switch is running VTP version 3, you can change to version 2 when the switch is in client mode if no extended VLANs exist, and no hidden password was configured.

Caution  VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

Caution  In TrCRF and TrBRF Token Ring environments, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, disable VTP version 2.

• In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

SUMMARY STEPS

1. enable
2. configure terminal
3. vtp version {1 | 2 | 3}
4. end
5. show vtp status
6. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vtp version {1</td>
<td>2</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Enabling VTP Pruning

#### Before you begin

VTP pruning is not designed to function in VTP transparent mode. If one or more switches in the network are in VTP transparent mode, you should do one of these actions:

- Turn off VTP pruning in the entire network.
- Turn off VTP pruning by making all VLANs on the trunk of the switch upstream to the VTP transparent switch pruning ineligible.

To configure VTP pruning on an interface, use the `switchport trunk pruning vlan` interface configuration command. VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `vtp pruning`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# vtp version 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show vtp status</td>
<td>Verifies that the configured VTP version is enabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show vtp status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- VTP Version, on page 1072
- VTP Version 2, on page 1069
- VTP Version 3, on page 1069
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; <code>enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables pruning in the VTP administrative domain.</td>
</tr>
<tr>
<td><code>vtp pruning</code></td>
<td>By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# <code>vtp pruning</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# <code>end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies your entries in the VTP Pruning Mode field of the display.</td>
</tr>
<tr>
<td><code>show vtp status</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <code>show vtp status</code></td>
</tr>
</tbody>
</table>

**Related Topics**

[VTP Pruning](#), on page 1070

### Configuring VTP on a Per-Port Basis

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic are blocked, not forwarded.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
**4. vtp**  
**5. end**  
**6. show running-config interface **interface-id**  
**7. show vtp status**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | |
| Example:                  | Enters global configuration mode. |
| Switch# configure terminal | |

| **Step 3** interface interface-id | |
| Example:                        | Identifies an interface, and enters interface configuration mode. |
| Switch(config)# interface gigabitethernet0/1 | |

| **Step 4** vtp | Enables VTP on the specified port. |
| Example:       | |
| Switch(config-if)# vtp | |

| **Step 5** end | Returns to privileged EXEC mode. |
| Example:       | |
| Switch(config)# end | |

| **Step 6** show running-config interface interface-id | Verifies the change to the port. |
| Example: | |
| Switch# show running-config interface gigabitethernet 0/1 | |

| **Step 7** show vtp status | Verifies the configuration. |
| Example:                  | |
| Switch# show vtp status | |
**Adding a VTP Client Switch to a VTP Domain**

Follow these steps to verify and reset the VTP configuration revision number on a switch before adding it to a VTP domain.

**Before you begin**

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is lower than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. With VTP versions 1 and 2, adding a switch that has a revision number higher than the revision number in the VTP domain can erase all VLAN information from the VTP server and VTP domain. With VTP version 3, the VLAN information is not erased.

You can use the `vtp mode transparent` global configuration command to disable VTP on the switch and then to change its VLAN information without affecting the other switches in the VTP domain.

**SUMMARY STEPS**

1. `enable`
2. `show vtp status`
3. `configure terminal`
4. `vtp domain domain-name`
5. `end`
6. `show vtp status`
7. `configure terminal`
8. `vtp domain domain-name`
9. `end`
10. `show vtp status`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><code>show vtp status</code></td>
<td>Checks the VTP configuration revision number.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show vtp status</code></td>
<td>If the number is 0, add the switch to the VTP domain.</td>
</tr>
<tr>
<td></td>
<td>If the number is greater than 0, follow these substeps:</td>
</tr>
<tr>
<td></td>
<td>• Write down the domain name.</td>
</tr>
<tr>
<td></td>
<td>• Write down the configuration revision number.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>3</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>4</td>
<td>vtp domain domain-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# vtp domain domain123</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>6</td>
<td>show vtp status</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# show vtp status</td>
</tr>
<tr>
<td>7</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>8</td>
<td>vtp domain domain-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# vtp domain domain012</td>
</tr>
<tr>
<td>9</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>10</td>
<td>show vtp status</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
</tbody>
</table>
Monitoring VTP

This section describes commands used to display and monitor the VTP configuration.

You monitor VTP by displaying VTP configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the switch.

Table 113: VTP Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show vtp counters</code></td>
<td>Displays counters about VTP messages that have been sent and received.</td>
</tr>
<tr>
<td><code>show vtp devices [conflict]</code></td>
<td>Displays information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The <code>show vtp devices</code> command does not display information when the switch is in transparent or off mode.</td>
</tr>
<tr>
<td><code>show vtp interface [interface-id]</code></td>
<td>Displays VTP status and configuration for all interfaces or the specified interface.</td>
</tr>
<tr>
<td><code>show vtp password</code></td>
<td>Displays the VTP password. The form of the password displayed depends on whether or not the <code>hidden</code> keyword was entered and if encryption is enabled on the switch.</td>
</tr>
<tr>
<td><code>show vtp status</code></td>
<td>Displays the VTP switch configuration information.</td>
</tr>
</tbody>
</table>

Configuration Examples for VTP

Example: Configuring a Switch as the Primary Server

This example shows how to configure a switch as the primary server for the VLAN database (the default) when a hidden or secret password was configured:
Switch# vtp primary vlan
VTP Feature Conf Revision Primary Server Device ID Device Description
------------ ---- -------- -------------- -------------- ----------------------
VLAN Yes 25 bcf1.f2e4.9700 0c75.bd07.4a00 P3A_NEW
VLAN Yes 547 0c75.bd07.4a00 40a6.e8db.9780 Switch_A
MST Yes 10 006c.bc4e.2500 40a6.e8db.9780 Switch_A
VLAN Yes 25 bcf1.f2e4.9700 e8b7.489c.cc00 Switch_B-11

Do you want to continue? [confirm]
Switch#

Jun 17 01:08:50.758 PST: %SW_VLAN-4-VTPPRIMARYSERVER_CHG: 006c.bc4e.2500 has become the
primary server for the VLAN VTP feature

Related Topics
   Configuring a VTP Version 3 Password, on page 1076
   Passwords for the VTP Domain, on page 1072

Example: Configuring Switch as VTP Server

This example shows how to configure the switch as a VTP server with the domain name eng_group and the
password mypassword:

Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.

Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.

Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end

Related Topics
   Configuring VTP Mode, on page 1074
   VTP Modes, on page 1067

Example: Enabling VTP on the Interface

To enable VTP on the interface, use the vtp interface configuration command. To disable VTP on the interface,
use the no vtp interface configuration command.

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# vtp
Switch(config-if)# end

Example: Creating the VTP Password

The follow is an example of creating the VTP password.

Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Where to Go Next

After configuring VTP, you can configure the following:

- VLANS
- VLAN Trunking
- VLAN Membership Policy Server (VMPS)
- Voice VLANs

Additional References

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>

Feature History and Information for VTP

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER

55

VLANs

• Finding Feature Information, on page 1087
• Prerequisites for VLANs, on page 1087
• Restrictions for VLANs, on page 1088
• Information About VLANs, on page 1088
• How to Configure VLANs, on page 1093
• Monitoring VLANs, on page 1100
• Configuration Examples, on page 1102
• Where to Go Next, on page 1103
• Additional References, on page 1103
• Feature History and Information for VLAN, on page 1104

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLANs

The following are prerequisites and considerations for configuring VLANs:

• Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network.

• The switch supports 1000 VLANs in VTP client, server, and transparent modes.
Restrictions for VLANs

The following are restrictions for configuring VLANs:

- 1K VLAN is supported only on switches running the LAN Base image with the lanbase-default template set.

- To avoid warning messages of high CPU utilization with a normal-range VLAN configuration, we recommend that you have no more than 256 VLANs. In such cases, approximately 10 access interfaces or 5 trunk interfaces can flap simultaneously with negligible impact to CPU utilization (if there are more interfaces that flap simultaneously, then CPU usage may be excessively high.)

Information About VLANs

Logical Networks

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or a switch supporting fallback bridging. Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of spanning tree.

VLANs are often associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Interface VLAN membership on the switch is assigned manually on an interface-by-interface basis. When you assign switch interfaces to VLANs by using this method, it is known as interface-based, or static, VLAN membership.

Traffic between VLANs must be routed.

The switch can route traffic between VLANs by using switch virtual interfaces (SVIs). An SVI must be explicitly configured and assigned an IP address to route traffic between VLANs.
Supported VLANs

The switch supports VLANs in VTP client, server, and transparent modes. VLANs are identified by a number from 1 to 4094. VLAN IDs 1002 through 1005 are reserved for Token Ring and FDDI VLANs.

VTP version 1 and version 2 support only normal-range VLANs (VLAN IDs 1 to 1005). In these versions, the switch must be in VTP transparent mode when you create VLAN IDs from 1006 to 4094. Cisco IOS Release 12.2(52)SE and later support VTP version 3. VTP version 3 supports the entire VLAN range (VLANs 1 to 4094). Extended range VLANs (VLANs 1006 to 4094) are supported only in VTP version 3. You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured in the domain.

Although the switch stack supports a total of 1,000 (normal range and extended range) VLANs, the number of configured features affects the use of the switch hardware.

The switch supports per-VLAN spanning-tree plus (PVST+) or rapid PVST+ with a maximum of 64 spanning-tree instances. One spanning-tree instance is allowed per VLAN. The switch supports only IEEE 802.1Q trunking methods for sending VLAN traffic over Ethernet ports.

VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that specifies the kind of traffic the port carries and the number of VLANs to which it can belong.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis.

Table 114: Port Membership Modes and Characteristics

<table>
<thead>
<tr>
<th>Membership Mode</th>
<th>VLAN Membership Characteristics</th>
<th>VTP Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static-access</td>
<td>A static-access port can belong to one VLAN and is manually assigned to that VLAN.</td>
<td>VTP is not required. If you do not want VTP to globally propagate information, set the VTP mode to transparent. To participate in VTP, there must be at least one trunk port on the switch connected to a trunk port of a second switch.</td>
</tr>
<tr>
<td>Trunk (IEEE 802.1Q): • IEEE 802.1Q—Industry-standard trunking encapsulation.</td>
<td>A trunk port is a member of all VLANs by default, including extended-range VLANs, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list.</td>
<td>VTP is recommended but not required. VTP maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links.</td>
</tr>
</tbody>
</table>
### Membership Mode | VLAN Membership Characteristics | VTP Characteristics
--- | --- | ---
Dynamic access | A dynamic-access port can belong to one VLAN (VLAN ID 1 to 4094) and is dynamically assigned by a VLAN Member Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch, for example, but never a Catalyst switch. The Catalyst switch is a VMPS client. You can have dynamic-access ports and trunk ports on the same switch, but you must connect the dynamic-access port to an end station or hub and not to another switch. | VTP is required. Configure the VMPS and the client with the same VTP domain name. To participate in VTP, at least one trunk port on the switch must be connected to a trunk port of a second switch.

Voice VLAN | A voice VLAN port is an access port attached to a Cisco IP Phone, configured to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. | VTP is not required; it has no effect on a voice VLAN.

---

### VLAN Configuration Files

Configurations for VLAN IDs 1 to 1005 are written to the vlan.dat file (VLAN database), and you can display them by entering the `show vlan` privileged EXEC command. The vlan.dat file is stored in flash memory. If the VTP mode is transparent, they are also saved in the switch running configuration file.

You use the interface configuration mode to define the port membership mode and to add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the `show running-config` privileged EXEC command.

When you save VLAN and VTP information (including extended-range VLAN configuration information) in the startup configuration file and reboot the switch, the switch configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration, and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration does not match the VLAN database, the domain name and VTP mode and configuration for the VLAN IDs 1 to 1005 use the VLAN database information.

- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for VLAN IDs 1 to 1005 use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.

- From image 15.0(02)SE6, on vtp transparent and off modes, vlans get created from startup-config even if they are not applied to the interface.

---

### Normal-Range VLAN Configuration Guidelines

Normal-range VLANs are VLANs with IDs from 1 to 1005.
VTP 1 and 2 only support normal-range VLANs.

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- Normal-range VLANs are identified with a number between 1 and 1001. VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs.

- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configurations are also saved in the switch running configuration file.

- If the switch is in VTP server or VTP transparent mode, you can add, modify or remove configurations for VLANs 2 to 1001 in the VLAN database. (VLAN IDs 1 and 1002 to 1005 are automatically created and cannot be removed.)

- With VTP versions 1 and 2, the switch supports VLAN IDs 1006 through 4094 only in VTP transparent mode (VTP disabled). These are extended-range VLANs and configuration options are limited. Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation in VTP server mode. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2.

- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. If the switch is a VTP server, you must define a VTP domain or VTP will not function.

- The switch does not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it does propagate the VLAN configuration through VTP.

- The switch supports 64 spanning tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 64 VLANs and is disabled on the remaining VLANs. If you have already used all available spanning-tree instances on a switch, adding another VLAN anywhere in the VTP domain creates a VLAN on that switch that is not running spanning-tree. If you have the default allowed list on the trunk ports of that switch (which is to allow all VLANs), the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that would not be broken, particularly if there are several adjacent switches that all have run out of spanning-tree instances. You can prevent this possibility by setting allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances.

If the number of VLANs on the switch exceeds the number of supported spanning-tree instances, we recommend that you configure the IEEE 802.1s Multiple STP (MSTP) on your switch to map multiple VLANs to a single spanning-tree instance.

Related Topics
- Creating or Modifying an Ethernet VLAN
- Deleting a VLAN, on page 1095
- Assigning Static-Access Ports to a VLAN
- Monitoring VLANs
- Example: Creating a VLAN Name, on page 1102

Extended-Range VLAN Configuration Guidelines

Extended-range VLANs are VLANs with IDs from 1006 to 4094.

VTP 3 only supports extended-range VLANs.

Follow these guidelines when creating extended-range VLANs:
• VLAN IDs in the extended range are not saved in the VLAN database and are not recognized by VTP unless the switch is running VTP version 3.

• You cannot include extended-range VLANs in the pruning eligible range.

• For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. You should save this configuration to the startup configuration so that the switch boots up in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets. If you create extended-range VLANs in VTP version 3, you cannot convert to VTP version 1 or 2.

• Although the switch stack supports a total of 1000 (normal-range and extended-range) VLANs, the number of configured features affects the use of the switch hardware. If you try to create an extended-range VLAN and there are not enough hardware resources available, an error message is generated, and the extended-range VLAN is rejected.

Related Topics
- Creating an Extended-Range VLAN
- Creating an Extended-Range VLAN with an Internal VLAN ID
- Monitoring VLANs
- Creating an Extended-Range VLAN, on page 1098
- Example: Creating an Extended-Range VLAN, on page 1103

Default VLAN Configurations

Default Ethernet VLAN Configuration

The following table displays the default configuration for Ethernet VLANs.

The switch supports Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1 to 4094.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>Extended-range VLANs (VLAN IDs 1006 to 4094) are only saved in the VLAN database in VTP version 3.</td>
</tr>
<tr>
<td>VLAN name</td>
<td>VLANxxxx, where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number</td>
<td>No range</td>
</tr>
</tbody>
</table>
Default VLAN Configuration

You can change only the MTU size and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

**Note**
The switch must be running the LAN Base image to support remote SPAN.

### How to Configure VLANs

#### How to Configure Normal-Range VLANs

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type
  - Ethernet
  - Fiber Distributed Data Interface [FDDI]
  - FDDI network entity title [NET]
  - TrBRF or TrCRF
  - Token Ring
  - Token Ring-Net
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.10 SAID</td>
<td>100001 (100000 plus the VLAN ID)</td>
<td>1 to 4294967294</td>
</tr>
<tr>
<td>IEEE 802.10 SAID</td>
<td>1500</td>
<td>576-18190</td>
</tr>
</tbody>
</table>
**Creating or Modifying an Ethernet VLAN**

Each Ethernet VLAN in the VLAN database has a unique, 4-digit ID that can be a number from 1 to 1001. VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs. To create a normal-range VLAN to be added to the VLAN database, assign a number and name to the VLAN.

---

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vlan vlan-id`
4. `name vlan-name`
5. `mtu mtu-size`
6. `end`
7. `show vlan {name vlan-name | id vlan-id}`
8. `copy running-config startup-config`

---

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Enters global configuration mode. |
| `configure terminal` | |
| **Example:** | |
| `Switch# configure terminal` | |

| **Step 3** | Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. |
| `vlan vlan-id` | |
| **Example:** | The available VLAN ID range for this command is 1 to 4094. |
| `Switch(config)# vlan 20` | Note |
### Deleting a VLAN

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from the VLAN database for all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

**Caution**

When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

### SUMMARY STEPS

1. enable
2. configure terminal
3. no vlan vlan-id
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Removes the VLAN by entering the VLAN ID.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>no vlan vlan-id</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# no vlan 4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies the VLAN removal.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>show vlan brief</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show vlan brief</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- Supported VLANs
- Normal-Range VLAN Configuration Guidelines, on page 1090
- Monitoring VLANs
Assigning Static-Access Ports to a VLAN

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information by disabling VTP (VTP transparent mode).

If you assign an interface to a VLAN that does not exist, the new VLAN is created.

SUMMARY STEPS

1. `configure terminal`
2. `interface interface-id`
3. `switchport mode access`
4. `switchport access vlan vlan-id`
5. `end`
6. `show running-config interface interface-id`
7. `show interfaces interface-id switchport`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Enters the interface to be added to the VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport mode access</td>
<td>Defines the VLAN membership mode for the port (Layer 2 access port).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport access vlan vlan-id</td>
<td>Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport access vlan 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### How to Configure Extended-Range VLANs

With VTP version 1 and version 2, when the switch is in VTP transparent mode (VTP disabled), you can create extended-range VLANs (in the range 1006 to 4094). VTP version supports extended-range VLANs in server or transparent move. Extended-range VLANs enable service providers to extend their infrastructure to a greater number of customers. The extended-range VLAN IDs are allowed for any `switchport` commands that allow VLAN IDs.

With VTP version 1 or 2, extended-range VLAN configurations are not stored in the VLAN database, but because VTP mode is transparent, they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file by using the `copy running-config startup-config` privileged EXEC command. Extended-range VLANs created in VTP version 3 are stored in the VLAN database.

### Creating an Extended-Range VLAN

You create an extended-range VLAN in global configuration mode by entering the `vlan` global configuration command with a VLAN ID from 1006 to 4094. The extended-range VLAN has the default Ethernet VLAN characteristics and the MTU size, and RSPAN configuration are the only parameters you can change. See the description of the `vlan` global configuration command in the command reference for the default settings of all parameters. In VTP version 1 or 2, if you enter an extended-range VLAN ID when the switch is not in VTP transparent mode, an error message is generated when you exit VLAN configuration mode, and the extended-range VLAN is not created.

In VTP version 1 and 2, extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the extended-range VLAN configuration in the switch startup configuration file by using the `copy running-config startup-config` privileged EXEC command. VTP version 3 saves extended-range VLANs in the VLAN database.

### SUMMARY STEPS

1. `configure terminal`
2. `vtp mode transparent`
3. `vlan vlan-id`
4. `mtu mtu size`
5. `remote-span`
6. `end`
7. `show vlan id vlan-id`
8. `copy running-config startup config`

## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configures the switch for VTP transparent mode, disabling VTP.</td>
</tr>
<tr>
<td><code>vtp mode transparent</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# vtp mode transparent</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This step is not required for VTP version 3.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.</td>
</tr>
<tr>
<td><code>vlan vlan-id</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# vlan 2000</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-vlan)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Modifies the VLAN by changing the MTU size.</td>
</tr>
<tr>
<td><code>mtu mtu size</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-vlan)# mtu 1024</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Configures the VLAN as the RSPAN VLAN.</td>
</tr>
<tr>
<td><code>remote-span</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-vlan)# remote-span</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Verifies that the VLAN has been created.</td>
</tr>
<tr>
<td><code>show vlan id vlan-id</code></td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring VLANs

#### Step 8

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch# show vlan id 2000</strong></td>
<td>Saves your entries in the switch startup configuration file. To save an extended-range VLAN configuration, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.</td>
</tr>
<tr>
<td><strong>copy running-config startup-config</strong></td>
<td>This step is not required for VTP version 3 because VLANs are saved in the VLAN database.</td>
</tr>
</tbody>
</table>

**Note**

- Related Topics
  - Extended-Range VLAN Configuration Guidelines, on page 1091
  - Example: Creating an Extended-Range VLAN, on page 1103

---

**Table 116: Privileged EXEC show Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show interfaces [vlan vlan-id]</strong></td>
<td>Displays characteristics for all interfaces or for the specified VLAN configured on the switch.</td>
</tr>
</tbody>
</table>
### Command

```
show vlan [brief | group [group-name name] | id vlan-id | ifindex | internal | mtu | name name | remote-span | summary]
```

### Purpose

Displays parameters for all VLANs or the specified VLAN on the switch. The following command options are available:

- **brief**—Displays VTP VLAN status in brief.
- **group**—Displays the VLAN group with its name and the connected VLANs that are available.
- **id**—Displays VTP VLAN status by identification number.
- **ifindex**—Displays SNMP ifIndex.
- **mtu**—Displays VLAN MTU information.
- **name**—Display the VTP VLAN information by specified name.
- **remote-span**—Displays the remote SPAN VLANs.
- **summary**—Displays a summary of VLAN information.
**Command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlan [ access-log {config</td>
<td>flow</td>
</tr>
<tr>
<td>Displays parameters for all VLANs or the specified VLAN on the switch. The following command options are available:</td>
<td></td>
</tr>
<tr>
<td>• access-log—Displays the VACL logging.</td>
<td></td>
</tr>
<tr>
<td>• access-map—Displays the VLAN access-maps.</td>
<td></td>
</tr>
<tr>
<td>• brief—Displays VTP VLAN status in brief.</td>
<td></td>
</tr>
<tr>
<td>• dot1q—Displays the dot1q parameters.</td>
<td></td>
</tr>
<tr>
<td>• filter—Displays VLAN filter information.</td>
<td></td>
</tr>
<tr>
<td>• group—Displays the VLAN group with its name and the connected VLANs that are available.</td>
<td></td>
</tr>
<tr>
<td>• id—Displays VTP VLAN status by identification number.</td>
<td></td>
</tr>
<tr>
<td>• ifindex—Displays SNMP ifIndex.</td>
<td></td>
</tr>
<tr>
<td>• mtu—Displays VLAN MTU information.</td>
<td></td>
</tr>
<tr>
<td>• name—Display the VTP VLAN information by specified name.</td>
<td></td>
</tr>
<tr>
<td>• private-vlan—Displays private VLAN information.</td>
<td></td>
</tr>
<tr>
<td>• remote-span—Displays the remote SPAN VLANs.</td>
<td></td>
</tr>
<tr>
<td>• summary—Displays a summary of VLAN information.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples

**Example: Creating a VLAN Name**

This example shows how to create Ethernet VLAN 20, name it test20, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

**Related Topics**

- Creating or Modifying an Ethernet VLAN
- Normal-Range VLAN Configuration Guidelines, on page 1090
Example: Configuring a Port as Access Port

This example shows how to configure a port as an access port in VLAN 2:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end

Related Topics
Assigning Static-Access Ports to a VLAN, on page 1097

Example: Creating an Extended-Range VLAN

This example shows how to create a new extended-range VLAN with all default characteristics, enter VLAN configuration mode, and save the new VLAN in the switch startup configuration file:

Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
Switch(config-vlan)# end
Switch# copy running-config startup config

Related Topics
Creating an Extended-Range VLAN, on page 1098
Extended-Range VLAN Configuration Guidelines, on page 1091

Where to Go Next

After configuring VLANs, you can configure the following:

• VLAN Trunking Protocol (VTP)
• VLAN trunks

Additional References

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for VLAN

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
Configuring VLAN Trunks

- Finding Feature Information, on page 1105
- Prerequisites for VLAN Trunks, on page 1105
- Information About VLAN Trunks, on page 1106
- How to Configure VLAN Trunks, on page 1109
- Configuration Examples for VLAN Trunking, on page 1122
- Where to Go Next, on page 1123
- Additional References, on page 1123
- Feature History and Information for VLAN Trunks, on page 1124

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VLAN Trunks

The IEEE 802.1Q trunks impose these limitations on the trunking strategy for a network:

- In a network of Cisco switches connected through IEEE 802.1Q trunks, the switches maintain one spanning-tree instance for each VLAN allowed on the trunks. Non-Cisco devices might support one spanning-tree instance for all VLANs.

When you connect a Cisco switch to a non-Cisco device through an IEEE 802.1Q trunk, the Cisco switch combines the spanning-tree instance of the VLAN of the trunk with the spanning-tree instance of the non-Cisco IEEE 802.1Q switch. However, spanning-tree information for each VLAN is maintained by Cisco switches separated by a cloud of non-Cisco IEEE 802.1Q switches. The non-Cisco IEEE 802.1Q cloud separating the Cisco switches is treated as a single trunk link between the switches.
• Make sure the native VLAN for an IEEE 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

• Disabling spanning tree on the native VLAN of an IEEE 802.1Q trunk without disabling spanning tree on every VLAN in the network can potentially cause spanning-tree loops. We recommend that you leave spanning tree enabled on the native VLAN of an IEEE 802.1Q trunk or disable spanning tree on every VLAN in the network. Make sure your network is loop-free before disabling spanning tree.

Information About VLAN Trunks

Trunking Overview

A trunk is a point-to-point link between one or more Ethernet switch interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

Note

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle.

Trunking Modes

Ethernet trunk interfaces support different trunking modes. You can set an interface as trunking or nontrunking or to negotiate trunking with the neighboring interface. To autonegotiate trunking, the interfaces must be in the same VTP domain.

Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a Point-to-Point Protocol (PPP). However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

Related Topics

Configuring a Trunk Port, on page 1109
Layer 2 Interface Modes, on page 1106

Layer 2 Interface Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport mode access</td>
<td>Puts the interface (access port) into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The interface becomes a nontrunk interface regardless of whether or not the neighboring interface is a trunk interface.</td>
</tr>
</tbody>
</table>
Function Mode

*switchport mode dynamic auto*

Makes the interface able to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk* or *desirable* mode. The default switchport mode for all Ethernet interfaces is *dynamic auto*.

*switchport mode dynamic desirable*

Makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to *trunk*, *desirable*, or *auto* mode.

*switchport mode trunk*

Puts the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. The interface becomes a trunk interface even if the neighboring interface is not a trunk interface.

*switchport nonegotiate*

Prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is *access* or *trunk*. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.

**Related Topics**

- Configuring a Trunk Port, on page 1109
- Trunking Modes, on page 1106

### Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), DTP, and VTP in VLAN 1.

If a trunk port with VLAN 1 disabled is converted to a nontrunk port, it is added to the access VLAN. If the access VLAN is set to 1, the port will be added to VLAN 1, regardless of the *switchport trunk allowed* setting. The same is true for any VLAN that has been disabled on the port.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

**Related Topics**

- Defining the Allowed VLANs on a Trunk, on page 1111
Load Sharing on Trunk Ports

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. Using load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

Network Load Sharing Using STP Priorities

When two ports on the same switch form a loop, the switch uses the STP port priority to decide which port is enabled and which port is in a blocking state. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port sends or receives all traffic for the VLAN.

Related Topics

Configuring Load Sharing Using STP Port Priorities, on page 1116

Network Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs, blocking different ports for different VLANs. The VLANs keep the traffic separate and maintain redundancy in the event of a lost link.

Related Topics

Configuring Load Sharing Using STP Path Cost, on page 1120

Feature Interactions

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.

- Trunk ports can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you entered to all ports in the group:
  - Allowed-VLAN list.
  - STP port priority for each VLAN.
  - STP Port Fast setting.
  - Trunk status:
    - If one port in a port group ceases to be a trunk, all ports cease to be trunks.

- We recommend that you configure no more than 24 trunk ports in Per VLAN Spanning Tree (PVST) mode and no more than 40 trunk ports in Multiple Spanning Tree (MST) mode.
• If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.

• A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable IEEE 802.1x on a dynamic port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, the port mode is not changed.

Default Layer 2 Ethernet Interface VLAN Configuration

The following table shows the default Layer 2 Ethernet interface VLAN configuration.

Table 118: Default Layer 2 Ethernet Interface VLAN Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface mode</td>
<td>switchport mode dynamic auto</td>
</tr>
<tr>
<td>Allowed VLAN range</td>
<td>VLANs 1 to 4094</td>
</tr>
<tr>
<td>VLAN range eligible for pruning</td>
<td>VLANs 2 to 1001</td>
</tr>
<tr>
<td>Default VLAN (for access ports)</td>
<td>VLAN 1</td>
</tr>
<tr>
<td>Native VLAN (for IEEE 802.1Q trunks)</td>
<td>VLAN 1</td>
</tr>
</tbody>
</table>

How to Configure VLAN Trunks

To avoid trunking misconfigurations, configure interfaces connected to devices that do not support DTP to not forward DTP frames, that is, to turn off DTP.

• If you do not intend to trunk across those links, use the switchport mode access interface configuration command to disable trunking.

• To enable trunking to a device that does not support DTP, use the switchport mode trunk and switchport nonegotiate interface configuration commands to cause the interface to become a trunk but not to generate DTP frames.

Configuring an Ethernet Interface as a Trunk Port

Configuring a Trunk Port

Because trunk ports send and receive VTP advertisements, to use VTP you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

SUMMARY STEPS

1. `enable`
2. configure terminal
3. interface interface-id
4. switchport mode {dynamic {auto | desirable} | trunk}
5. switchport access vlan vlan-id
6. switchport trunk native vlan vlan-id
7. end
8. show interfaces interface-id switchport
9. show interfaces interface-id trunk
10. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the port to be configured for trunking, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface gigabitethernet 0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode {dynamic {auto</td>
<td>desirable}</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# switchport mode dynamic desirable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport access vlan vlan-id</td>
<td>(Optional) Specifies the default VLAN, which is used if the interface stops trunking.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Switch(config-if)# switchport access vlan 200**

**Purpose**

Specifies the native VLAN for IEEE 802.1Q trunks.

---

**Step 6**

**switchport trunk native vlan vlan-id**

*Example:*

```
Switch(config-if)# switchport trunk native vlan 200
```

**Step 7**

```
end
```

*Example:*

```
Switch(config)# end
```

**Step 8**

**show interfaces interface-id switchport**

*Example:*

```
Switch# show interfaces gigabitethernet 0/2 switchport
```

**Step 9**

**show interfaces interface-id trunk**

*Example:*

```
Switch# show interfaces gigabitethernet 0/2 trunk
```

**Step 10**

**copy running-config startup-config**

*Example:*

```
Switch# copy running-config startup-config
```

---

**Related Topics**

- [Trunking Modes](#)
- [Layer 2 Interface Modes](#)

---

**Defining the Allowed VLANs on a Trunk**

VLAN 1 is the default VLAN on all trunk ports in all Cisco switches, and it has previously been a requirement that VLAN 1 always be enabled on every trunk link. You can use the VLAN 1 minimization feature to disable VLAN 1 on any individual VLAN trunk link so that no user traffic (including spanning-tree advertisements) is sent or received on VLAN 1.
**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-id
4. switchport mode trunk
5. switchport trunk allowed vlan {add | all | except | remove} vlan-list
6. end
7. show interfaces interface-id switchport
8. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode trunk</td>
<td>Configures the interface as a VLAN trunk port.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport trunk allowed vlan {add</td>
<td>all</td>
</tr>
<tr>
<td>Example: Switch(config-if)# switchport trunk allowed vlan remove 2</td>
<td>The <em>vlan-list</em> parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges. All VLANs are allowed by default.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Related Topics

- **Allowed VLANs on a Trunk**, on page 1107

### Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `switchport trunk pruning vlan [add | except | none | remove] vlan-list [vlan [,vlan [...]]]`
5. `end`
6. `show interfaces interface-id switchport`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Selects the trunk port for which VLANs should be pruned, and enters interface configuration mode.</td>
</tr>
</tbody>
</table>

### Step 3

#### Example:

Switch(config)# interface fastethernet0/1-48

### Step 4

#### Example:

Switch(config)# interface fastethernet0/1-48

### Step 5

#### Example:

Switch(config)# end

### Step 6

#### Example:

Switch# show interfaces gigabitethernet 0/1 switchport

### Step 7

#### Example:

Switch# copy running-config startup-config

### Configuring the Native VLAN for Untagged Traffic

A trunk port configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic in the native VLAN configured for the port. The native VLAN is VLAN 1 by default.

The native VLAN can be assigned any VLAN ID.
If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the packet is sent untagged; otherwise, the switch sends the packet with a tag.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `switchport trunk native vlan vlan-id`
5. `end`
6. `show interfaces interface-id switchport`
7. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; <code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface interface-id</code></td>
<td>Defines the interface that is configured as the IEEE 802.1Q trunk, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>interface gigabitethernet 0/2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>switchport trunk native vlan vlan-id</code></td>
<td>Configures the VLAN that is sending and receiving untagged traffic on the trunk port. For <code>vlan-id</code>, the range is 1 to 4094.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <code>switchport trunk native vlan 12</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>show interfaces interface-id switchport</code></td>
<td>Verifies your entries in the <em>Trunking Native Mode VLAN</em> field.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Trunk Ports for Load Sharing

#### Configuring Load Sharing Using STP Port Priorities

These steps describe how to configure a network with load sharing using STP port priorities.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `vtp domain domain-name`
4. `vtp mode server`
5. `end`
6. `show vtp status`
7. `show vlan`
8. `configure terminal`
9. `interface interface-id`
10. `switchport mode trunk`
11. `end`
12. `show interfaces interface-id switchport`
13. Repeat the above steps on Switch A for a second port in the switch.
14. Repeat the above steps on Switch B to configure the trunk ports that connect to the trunk ports configured on Switch A.
15. `show vlan`
16. `configure terminal`
17. `interface interface-id`
18. `spanning-tree vlan vlan-range port-priority priority-value`
19. `exit`
20. `interface interface-id`
21. `spanning-tree vlan vlan-range port-priority priority-value`
22. `end`
23. `show running-config`
24. `copy running-config startup-config`

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch# show interfaces gigabitethernet 0/2 switchport</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode on Switch A.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vtp domain domain-name</td>
<td>Configures a VTP administrative domain.</td>
</tr>
<tr>
<td>Example: Switch(config)# vtp domain workdomain</td>
<td>The domain name can be 1 to 32 characters.</td>
</tr>
<tr>
<td><strong>Step 4</strong> vtp mode server</td>
<td>Configures Switch A as the VTP server.</td>
</tr>
<tr>
<td>Example: Switch(config)# vtp mode server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show vtp status</td>
<td>Verifies the VTP configuration on both Switch A and Switch B.</td>
</tr>
<tr>
<td>Example: Switch# show vtp status</td>
<td>In the display, check the VTP Operating Mode and the VTP Domain Name fields.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show vlan</td>
<td>Verifies that the VLANs exist in the database on Switch A.</td>
</tr>
<tr>
<td>Example: Switch# show vlan</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td><code>interface interface-id</code></td>
<td>Defines the interface to be configured as a trunk, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface fastethernet0/1-48</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>switchport mode trunk</code></td>
<td>Configures the port as a trunk port.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# switchport mode trunk</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# end</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>show interfaces interface-id switchport</code></td>
<td>Verifies the VLAN configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show interfaces gigabitethernet 0/1 switchport</code></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Repeat the above steps on Switch A for a second port in the switch.</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Repeat the above steps on Switch B to configure the trunk ports that connect to the trunk ports configured on Switch A.</td>
<td>When the trunk links come up, VTP passes the VTP and VLAN information to Switch B. This command verifies that Switch B has learned the VLAN configuration.</td>
</tr>
<tr>
<td>15</td>
<td><code>show vlan</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show vlan</code></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode on Switch A.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td><code>interface interface-id</code></td>
<td>Defines the interface to set the STP port priority, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 18</th>
<th>spanning-tree vlan vlan-range port-priority priority-value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# spanning-tree vlan 8-10 port-priority 16</td>
</tr>
</tbody>
</table>

Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.

<table>
<thead>
<tr>
<th>Step 19</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# exit</td>
</tr>
</tbody>
</table>

Returns to global configuration mode.

<table>
<thead>
<tr>
<th>Step 20</th>
<th>interface interface-id</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# interface gigabitethernet 0/2</td>
</tr>
</tbody>
</table>

Defines the interface to set the STP port priority, and enters interface configuration mode.

<table>
<thead>
<tr>
<th>Step 21</th>
<th>spanning-tree vlan vlan-range port-priority priority-value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# spanning-tree vlan 3-6 port-priority 16</td>
</tr>
</tbody>
</table>

Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.

<table>
<thead>
<tr>
<th>Step 22</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# end</td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.

<table>
<thead>
<tr>
<th>Step 23</th>
<th>show running-config</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show running-config</td>
</tr>
</tbody>
</table>

Verifies your entries.

<table>
<thead>
<tr>
<th>Step 24</th>
<th>copy running-config startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

(Optional) Saves your entries in the configuration file.

---

**Related Topics**

*Network Load Sharing Using STP Priorities*, on page 1108
Configuring Load Sharing Using STP Path Cost

These steps describe how to configure a network with load sharing using STP path costs.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-id
4. switchport mode trunk
5. exit
6. Repeat Steps 2 through 4 on a second interface in Switch A.
7. end
8. show running-config
9. show vlan
10. configure terminal
11. interface interface-id
12. spanning-tree vlan vlan-range cost cost-value
13. end
14. Repeat Steps 9 through 13 on the other configured trunk interface on Switch A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.
15. exit
16. show running-config
17. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode on Switch A.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Defines the interface to be configured as a trunk, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode trunk</td>
<td>Configures the port as a trunk port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode trunk</code></td>
<td>Verifies your entries. In the display, make sure that the interfaces are configured as trunk ports.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>When the trunk links come up, Switch A receives the VTP information from the other switches. This command verifies that Switch A has learned the VLAN configuration.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td>Defines the interface on which to set the STP cost, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Sets the spanning-tree path cost to 30 for VLANs 2 through 4.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><code>Example:</code></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td><code>Example:</code></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td><code>spanning-tree vlan vlan-range cost cost-value</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>Example:</code></td>
</tr>
<tr>
<td><code>end</code></td>
<td><code>Switch(config-if)# spanning-tree vlan 2-4 cost 30</code></td>
</tr>
<tr>
<td><code>Example:</code></td>
<td><code>Switch# show vlan</code></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td><code>Step 10</code></td>
</tr>
<tr>
<td><code>Step 8</code></td>
<td><code>Step 11</code></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Repeat Steps 9 through 13 on the other configured trunk interface on Switch A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td><strong>show running-config</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

Network Load Sharing Using STP Path Cost, on page 1108

## Configuration Examples for VLAN Trunking

### Example: Configuring a Trunk Port

The following example shows how to configure a port as an IEEE 802.1Q trunk. The example assumes that the neighbor interface is configured to support IEEE 802.1Q trunks.

```bash
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# end
```
Example: Removing a VLAN from a Port

This example shows how to remove VLAN 2 from the allowed VLAN list on a port:

Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end

Where to Go Next

After configuring VLAN trunks, you can configure the following:

• VLANs

Additional References

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature History and Information for VLAN Trunks

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)E</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for VMPS

You should configure the VLAN Membership Policy Server (VMPS) before you configure ports as dynamic-access ports.

When you configure a port as a dynamic-access port, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state. The VTP management domain of the VMPS client and the VMPS server must be the same.
Restrictions for VMPS

The following are restrictions for configuring VMPS:

- IEEE 802.1x ports cannot be configured as dynamic-access ports. If you try to enable IEEE 802.1x on a dynamic-access (VQP) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic-access ports, but you can enter the `switchport access vlan dynamic` interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port. You must turn off trunking on the port before the dynamic-access setting takes effect.
- Dynamic-access ports cannot be monitor ports.
- Secure ports cannot be dynamic-access ports. You must disable port security on a port before it becomes dynamic.
- Dynamic-access ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic-access ports.
- The VLAN configured on the VMPS server should not be a voice VLAN.
- 1K VLAN is supported only on switches running the LAN Base image with the lanbase-default template set.

Information About VMPS

Dynamic VLAN Assignments

The VLAN Query Protocol (VQP) is used to support dynamic-access ports, which are not permanently assigned to a VLAN, but give VLAN assignments based on the MAC source addresses seen on the port. Each time an unknown MAC address is seen, the switch sends a VQP query to a remote VLAN Membership Policy Server (VMPS); the query includes the newly seen MAC address and the port on which it was seen. The VMPS responds with a VLAN assignment for the port. The switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

Each time the client switch receives the MAC address of a new host, it sends a VQP query to the VMPS. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in open or secure mode. In secure mode, the server shuts down the port when an illegal host is detected. In open mode, the server denies the host access to the port.

If the port is currently unassigned (that is, it does not yet have a VLAN assignment), the VMPS provides one of these responses:

- If the host is allowed on the port, the VMPS sends the client a vlan-assignment response containing the assigned VLAN name and allowing access to the host.
• If the host is not allowed on the port and the VMPS is in open mode, the VMPS sends an access-denied response.

• If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a port-shutdown response.

If the port already has a VLAN assignment, the VMPS provides one of these responses:

• If the VLAN in the database matches the current VLAN on the port, the VMPS sends a success response, allowing access to the host.

• If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an access-denied or a port-shutdown response, depending on the secure mode of the VMPS.

If the switch receives an access-denied response from the VMPS, it continues to block traffic to and from the host MAC address. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new host address. If the switch receives a port-shutdown response from the VMPS, it disables the port. The port must be manually reenabled by using Network Assistant, the CLI, or SNMP.

Related Topics
- Configuring Dynamic-Access Ports on VMPS Clients, on page 1129
- Example: VMPS Configuration, on page 1135

Dynamic-Access Port VLAN Membership

A dynamic-access port can belong to only one VLAN with an ID from 1 to 4094. When the link comes up, the switch does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic-access port and attempts to match the MAC address to a VLAN in the VMPS database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic-access port if they are all in the same VLAN; however, the VMPS shuts down a dynamic-access port if more than 20 hosts are active on the port.

If the link goes down on a dynamic-access port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.

Dynamic-access ports can be used for direct host connections, or they can connect to a network. A maximum of 20 MAC addresses are allowed per port on the switch. A dynamic-access port can belong to only one VLAN at a time, but the VLAN can change over time, depending on the MAC addresses seen.

Related Topics
- Configuring Dynamic-Access Ports on VMPS Clients, on page 1129
- Example: VMPS Configuration, on page 1135
Default VMPS Client Configuration

The following table shows the default VMPS and dynamic-access port configuration on client switches.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMPS domain server</td>
<td>None</td>
</tr>
<tr>
<td>VMPS reconfirm interval</td>
<td>60 minutes</td>
</tr>
<tr>
<td>VMPS server retry count</td>
<td>3</td>
</tr>
<tr>
<td>Dynamic-access ports</td>
<td>None configured</td>
</tr>
</tbody>
</table>

How to Configure VMPS

Entering the IP Address of the VMPS

Note

If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Before you begin

You must first enter the IP address of the server to configure the switch as a client.

SUMMARY STEPS

1. enable
2. configure terminal
3. vmps server ipaddress primary
4. vmps server ipaddress
5. end
6. show vmps
7. copy running-config startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vmps server <em>ipaddress</em> primary</td>
<td>Enters the IP address of the switch acting as the primary VMPS server.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# vmps server 10.1.2.3 primary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vmps server <em>ipaddress</em></td>
<td>(Optional) Enters the IP address of the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# vmps server 10.3.4.5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show vmps</td>
<td>Verifies your entries in the VMPS Domain Server field of the display.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show vmps</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Dynamic-Access Ports on VMPS Clients

**Caution**

Dynamic-access port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic-access ports to other switches can cause a loss of connectivity.

If you are configuring a port on a cluster member switch as a dynamic-access port, first use the `rcommand` privileged EXEC command to log in to the cluster member switch.
Before you begin

You must have IP connectivity to the VMPS for dynamic-access ports to work. You can test for IP connectivity by pinging the IP address of the VMPS and verifying that you get a response.

**Note**

To return an interface to its default configuration, use the `default interface interface-id` interface configuration command. To return an interface to its default switchport mode (dynamic auto), use the `no switchport mode` interface configuration command. To reset the access mode to the default VLAN for the switch, use the `no switchport access vlan` interface configuration command.

---

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `interface interface-id`
4. `switchport mode access`
5. `switchport access vlan dynamic`
6. `end`
7. `show interfaces interface-id switchport`
8. `copy running-config startup-config`

---

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface interface-id</code></td>
<td>Specifies the switch port that is connected to the end station, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 1/0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>switchport mode access</code></td>
<td>Sets the port to access mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport mode access</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose
- **Configure the port as eligible for dynamic VLAN membership.**

### Command or Action
- `switchport access vlan dynamic`

### Example:
- `Switch(config-if)# switchport access vlan dynamic`

### Step 5
- **Thedynamic-accessportmustbeconnectedtoanendstation.**

### Command or Action
- `end`

### Example:
- `Switch(config)# end`

### Step 6
- **Returns to privileged EXEC mode.**

### Command or Action
- `show interfaces interface-id switchport`

### Example:
- `Switch# show interfaces gigabitethernet 1/0/1 switchport`

### Step 7
- **Verifies your entries in the Operational Mode field of the display.**

### Command or Action
- `copy running-config startup-config`

### Example:
- `Switch# copy running-config startup-config`

### Step 8
- **(Optional) Saves your entries in the configuration file.**

### Related Topics
- Dynamic VLAN Assignments, on page 1126
- Dynamic-Access Port VLAN Membership, on page 1127
- Example: VMPS Configuration, on page 1135

### Reconfirming VLAN Memberships

This task confirms the dynamic-access port VLAN membership assignments that the switch has received from the VMPS.

### SUMMARY STEPS
1. `enable`
2. `vmps reconfirm`
3. `show vmps`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
## Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs.

### Note

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command switch. You also must first use the `rcommand` privileged EXEC command to log in to the member switch.

### SUMMARY STEPS

1. enable
2. configure terminal
3. vmps reconfirm minutes
4. end
5. show vmps
6. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Changing the Retry Count

Follow these steps to change the number of times that the switch attempts to contact the VMPS before querying the next server.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. vmps retry count
4. end
5. show vmps
6. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Sets the number of minutes between reconfirmations of the dynamic VLAN membership. The range is 1 to 120. The default is 60 minutes.

Example:

Switch(config)# vmps reconfirm 90

Returns to privileged EXEC mode.

Example:

Switch(config)# end

Verifies the dynamic VLAN reconfirmation status in the Reconfirm Interval field of the display.

Example:

Switch# show vmps

(Optional) Saves your entries in the configuration file.

Example:

Switch# copy running-config startup-config
### Troubleshooting Dynamic-Access Port VLAN Membership

**Problem** The VMPS shuts down a dynamic-access port under these conditions:

- **Problem** The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- **Problem** More than 20 active hosts reside on a dynamic-access port.

**Solution** To reenable a disabled dynamic-access port, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.
Monitoring the VMPS

You can display information about the VMPS by using the `show vmps` privileged EXEC command. The switch displays this information about the VMPS:

- VMPS VQP Version—The version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP Version 1.
- Reconfirm Interval—The number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.
- Server Retry Count—The number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.
- VMPS domain server—The IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked `current`. The one marked `primary` is the primary server.
- VMPS Action—The result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expires, or you can force it by entering the `vmps reconfirm` privileged EXEC command or its Network Assistant or SNMP equivalent.

This is an example of output for the `show vmps` privileged EXEC command:

```
Switch# show vmps
VQP Client Status:
-------------------
VMPS VQP Version:  1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
172.20.128.87

Reconfirmation status
---------------------
VMPS Action: other
```

Configuration Example for VMPS

Example: VMPS Configuration

`Figure 62: Dynamic Port VLAN Membership Configuration`

This network has a VMPS server switch and VMPS client switches with dynamic-access ports with this configuration:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 6500 series Switch A is the primary VMPS server.
- The Catalyst 6500 series Switch C and Switch J are secondary VMPS servers.
- End stations are connected to the clients, Switch B and Switch I.
• The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.

Related Topics
- Configuring Dynamic-Access Ports on VMPS Clients, on page 1129
- Dynamic VLAN Assignments, on page 1126
- Dynamic-Access Port VLAN Membership, on page 1127

Where to Go Next

You can configure the following:
- VTP
- VLANs
• VLAN Trunking
• Voice VLANs

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>Catalyst 2960-X Switch VLAN Management Command Reference</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

Feature History and Information for VMPS

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td></td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Voice VLANs

The following are the prerequisites for voice VLANs:

- Voice VLAN configuration is only supported on switch access ports; voice VLAN configuration is not supported on trunk ports.

Note: Trunk ports can carry any number of voice VLANs, similar to regular VLANs. The configuration of voice VLANs is not supported on trunk ports.
Before you enable voice VLAN, we recommend that you enable QoS on the switch by entering the `mls qos` global configuration command and configure the port trust state to trust by entering the `mls qos trust cos` interface configuration command.

You must enable CDP on the switch port connected to the Cisco IP Phone to send the configuration to the phone. (CDP is globally enabled by default on all switch interfaces.)

**Restrictions for Voice VLANs**

You cannot configure static secure MAC addresses in the voice VLAN.

**Information About Voice VLAN**

**Voice VLANs**

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. When the switch is connected to a Cisco IP Phone, the phone sends voice traffic with Layer 3 IP precedence and Layer 2 class of service (CoS) values, which are both set to 5 by default. Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS) based on IEEE 802.1p CoS. QoS uses classification and scheduling to send network traffic from the switch in a predictable manner.

The Cisco IP Phone is a configurable device, and you can configure it to forward traffic with an IEEE 802.1p priority. You can configure the switch to trust or override the traffic priority assigned by a Cisco IP Phone.

**Cisco IP Phone Voice Traffic**

You can 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. You can configure access ports on the switch to send Cisco Discovery Protocol (CDP) packets that instruct an attached phone to send voice traffic to the switch in any of these ways:

- In the voice VLAN tagged with a Layer 2 CoS priority value
- In the access VLAN tagged with a Layer 2 CoS priority value
- In the access VLAN, untagged (no Layer 2 CoS priority value)

In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5 for voice traffic and 3 for voice control traffic).

**Related Topics**

- Configuring Cisco IP Phone Voice Traffic
- Example: Configuring Cisco IP Phone Voice Traffic, on page 1144
Cisco IP Phone Data Traffic

The switch can also process tagged data traffic (traffic in IEEE 802.1Q or IEEE 802.1p frame types) from the device attached to the access port on the Cisco IP Phone. You can configure Layer 2 access ports on the switch to send CDP packets that instruct the attached phone to configure the phone access port in one of these modes:

• In trusted mode, all traffic received through the access port on the Cisco IP Phone passes through the phone unchanged.

• In untrusted mode, all traffic in IEEE 802.1Q or IEEE 802.1p frames received through the access port on the Cisco IP Phone receive a configured Layer 2 CoS value. The default Layer 2 CoS value is 0. Untrusted mode is the default.

Note

Untagged traffic from the device attached to the Cisco IP Phone passes through the phone unchanged, regardless of the trust state of the access port on the phone.

Voice VLAN Configuration Guidelines

• Because a Cisco IP Phone also supports a connection to a PC or other device, a port connecting the switch to a Cisco IP Phone can carry mixed traffic. You can configure a port to decide how the Cisco IP Phone carries voice traffic and data traffic.

• The voice VLAN should be present and active on the switch for the IP phone to correctly communicate on the voice VLAN. Use the `show vlan` privileged EXEC command to see if the VLAN is present (listed in the display). If the VLAN is not listed, create the voice VLAN.

• The Power over Ethernet (PoE) switches are capable of automatically providing power to Cisco pre-standard and IEEE 802.3af-compliant powered devices if they are not being powered by an AC power source.

• The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

• If the Cisco IP Phone and a device attached to the phone are in the same VLAN, they must be in the same IP subnet. These conditions indicate that they are in the same VLAN:
  • They both use IEEE 802.1p or untagged frames.
  • The Cisco IP Phone uses IEEE 802.1p frames, and the device uses untagged frames.
  • The Cisco IP Phone uses untagged frames, and the device uses IEEE 802.1p frames.
  • The Cisco IP Phone uses IEEE 802.1Q frames, and the voice VLAN is the same as the access VLAN.

• The Cisco IP Phone and a device attached to the phone cannot communicate if they are in the same VLAN and subnet but use different frame types because traffic in the same subnet is not routed (routing would eliminate the frame type difference).

• Voice VLAN ports can also be these port types:
  • Dynamic access port.
  • IEEE 802.1x authenticated port.
If you enable IEEE 802.1x on an access port on which a voice VLAN is configured and to which a Cisco IP Phone is connected, the phone loses connectivity to the switch for up to 30 seconds.

- Protected port.
- A source or destination port for a SPAN session.
- Secure port.

When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP Phone, the phone requires up to two MAC addresses. The phone address is learned on the voice VLAN and might also be learned on the access VLAN. Connecting a PC to the phone requires additional MAC addresses.

Default Voice VLAN Configuration

The voice VLAN feature is disabled by default.

When the voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port.

The CoS value is not trusted for IEEE 802.1p or IEEE 802.1Q tagged traffic.

How to Configure Voice VLAN

Configuring Cisco IP Phone Voice Traffic

You can configure a port connected to the Cisco IP Phone to send CDP packets to the phone to configure the way in which the phone sends voice traffic. The phone can carry voice traffic in IEEE 802.1Q frames for a specified voice VLAN with a Layer 2 CoS value. It can use IEEE 802.1p priority tagging to give voice traffic a higher priority and forward all voice traffic through the native (access) VLAN. The Cisco IP Phone can also send untagged voice traffic or use its own configuration to send voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. mls qos trust cos
5. `switchport voice {vlan|dot1p|none|untagged}`
6. `end`
7. Use one of the following:
   - `show interfaces interface-id switchport`
   - `show running-config interface interface-id`
8. `copy running-config startup-config`

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>interface interface-id</code></td>
<td>Specifies the interface connected to the phone, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>mls qos trust cos</code></td>
<td>Configures the interface to classify incoming traffic packets by using the packet CoS value. For untagged packets, the port default CoS value is used.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# mls qos trust cos</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>`switchport voice {vlan</td>
<td>dot1p</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# switchport voice vlan dot1p</code></td>
<td>• <code>vlan-id</code>—Configures the phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP Phone forwards the voice traffic with an IEEE 802.1Q priority of 5. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dot1p</code>—Configures the switch to accept voice and data IEEE 802.1p priority frames tagged with VLAN ID 0 (the native VLAN). By default, the switch drops all voice and data traffic tagged with VLAN 0. If configured for 802.1p the Cisco IP Phone forwards the traffic with an IEEE 802.1p priority of 5.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>none</strong></td>
<td>Allows the phone to use its own configuration to send untagged voice traffic.</td>
</tr>
<tr>
<td>• <strong>untagged</strong></td>
<td>Configures the phone to send untagged voice traffic.</td>
</tr>
</tbody>
</table>

### Step 6

**end**

Example:

```
Switch(config-if)# end
```

Returns to privileged EXEC mode.

### Step 7

Use one of the following:

- `show interfaces interface-id switchport`
- `show running-config interface interface-id`

Example:

```
Switch# show interfaces gigabitethernet 0/1
switchport
```

or

```
Switch# show running-config interface gigabitethernet 0/1
```

Verifies your voice VLAN entries or your QoS and voice VLAN entries.

### Step 8

`copy running-config startup-config`

Example:

```
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

---

**Monitoring Voice VLAN**

To display voice VLAN configuration for an interface, use the `show interfaces interface-id switchport` privileged EXEC command.

### Configuration Examples

#### Example: Configuring Cisco IP Phone Voice Traffic

This example shows how to configure a port connected to a Cisco IP Phone to use the CoS value to classify incoming traffic and to accept voice and data priority traffic tagged with VLAN ID 0:
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end

To return the port to its default setting, use the no switchport voice vlan interface configuration command.

Related Topics
    Configuring Cisco IP Phone Voice Traffic
    Cisco IP Phone Voice Traffic, on page 1140

Where to Go Next
After configuring voice VLANs, you can configure the following:

• VLANs
• VLAN Trunking
• VTP

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>For complete syntax and usage information for the commands used in this chapter.</td>
<td>Catalyst 2960-L Switch VLAN Management Command Reference</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature History and Information for Voice VLAN

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.0(2)EX</td>
<td>Cisco IOS Release 15.2(5)E</td>
</tr>
<tr>
<td>This feature was introduced.</td>
<td></td>
</tr>
</tbody>
</table>
Important Notice

- Disclaimer, on page 1147
- Statement 361—VoIP and Emergency Calling Services do not Function if Power Fails, on page 1147
- Statement 1071—Warning Definition, on page 1149

Disclaimer

Cisco EnergyWise enables you to reduce energy consumption in your network by turning off the power to devices when they are not in use. If IP phones are part of your network, they can also be turned off through EnergyWise, in which case calls cannot be made or received, and the phones cannot be turned on except by the network administrator or according to rules established in EnergyWise by the network administrator. Laws in the location of your network might require phones to remain available for emergencies. It is your responsibility to identify the laws that apply and to comply with them. Even in the absence of a law, we strongly recommend that you designate certain phones that will always be on and available to make and receive emergency calls. These phones should be clearly identified, and all employees or others who might require emergency access to make or receive calls should be informed of the availability of these phones.

Statement 361—VoIP and Emergency Calling Services do not Function if Power Fails

<table>
<thead>
<tr>
<th></th>
<th>Voice over IP (VoIP) service and the emergency calling service do not function if power fails or is disrupted. After power is restored, you might have to reset or reconfigure equipment to regain access to VoIP and the emergency calling service. In the USA, this emergency number is 911. You need to be aware of the emergency number in your country.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waarschuwing</td>
<td>Voice over IP (VoIP)-service en de service voor noodoproepen werken niet indien er een stroomstoring is. Nadat de stroomteweer is hersteld, dient u wellicht de configuratie van uw apparatuur opnieuw in te stellen om opnieuw toegang te krijgen tot VoIP en de noodoproepen. In de VS is het nummer voor noodoproepen 911. U dient u zelf op de hoogte te stellen van het nummer voor noodoproepen in uw land.</td>
</tr>
<tr>
<td>Attention</td>
<td>Le service Voice over IP (VoIP) et le service d'appels d'urgence ne fonctionnent pas en cas de panne de courant. Une fois que le courant est rétabli, vous devrez peut-être réinitialiser ou reconfigurer le système pour accéder de nouveau au service VoIP et à celui des appels d'urgence. Aux États-Unis, le numéro des services d'urgence est le 911. Vous devez connaître le numéro d’appel d’urgence en vigueur dans votre pays.</td>
</tr>
<tr>
<td>Avvertenza</td>
<td>Il servizio Voice over IP (VoIP) e il servizio per le chiamate di emergenza non funziona in caso di interruzione dell'alimentazione. Ristabilita l'alimentazione, potrebbe essere necessario reimpostare o reconfigurare l'attrezzatura per ottenere nuovamente l'accesso al servizio VoIP e al servizio per le chiamate di emergenza. Negli Stati Uniti, il numero di emergenza è 911. Si consiglia di individuare il numero di emergenza del proprio Paese.</td>
</tr>
<tr>
<td>Aviso</td>
<td>O serviço Voice over IP (VoIP) e o serviço de chamadas de emergência não funcionam se houver um corte de energia. Depois do fornecimento de energia ser restabelecido, poderá ser necessário reiniciar ou reconfigurar o equipamento para voltar a utilizar os serviços VoIP ou chamadas de emergência. Nos EUA, o número de emergência é o 911. É importante que saiba qual o número de emergência no seu país.</td>
</tr>
<tr>
<td>¡Advertencia!</td>
<td>El servicio de voz sobre IP (VoIP) y el de llamadas de emergencia no funcionan si se interrumpe el suministro de energía. Tras recuperar el suministro es posible que deba que restablecer o volver a configurar el equipo para tener acceso a los servicios de VoIP y de llamadas de emergencia. En Estados Unidos el número de emergencia es el 911. Asegúrese de obtener el número de emergencia en su país.</td>
</tr>
</tbody>
</table>
Varning!

Figyellem
Az IP csatornán történő hangátvitel (VoIP) és a segélyhívó szolgáltatás nem működik, ha az áramellátás megszűnik vagy megszakad. Az áramellátás helyreállítását követően előfordulhat, hogy alaphelyzetbe kell állítani vagy újra kell konfigurálni a berendezést, hogy újra hozzáférhessen a VoIP és a segélyhívó szolgáltatáshoz. Az Egyesült Államokban a segélyhívó szám 911. Tisztában kell lennie a saját országának segélyhívó számával.

Предупреждение
Служба передачи голоса по IP (VoIP) и служба электронных вызовов не будут работать, если произошел сбой питания. После восстановления питания, возможно, потребуется перенастроить оборудование, чтобы возобновить доступ к службе VoIP и службе электронных вызовов. В США телефон службы электронных вызовов 911. Вам необходимо знать телефон этой службы в своей стране.

警告
如果电源出现故障或中断，您将无法使用Voice over IP (VoIP)服务与紧急呼叫服务。电源恢复之后，您可能需要重新设置或重新配置设备，以便重新获得VoIP和紧急呼叫服务的权限。在美国，此紧急呼叫号码是911。您必须知道本国的紧急呼叫号码。

警告
電源障害や停電の場合、ボイス オーバー インターネット (VoIP) サービスと緊急通報サービスは機能しません。電源の回復後、VoIPと緊急通報サービスへのアクセスには機器をリセットまたは再設定する必要があります。米国内の緊急通報番号は911です。お住まいの地域の緊急通報番号をお知らせしておいてください。

Statement 1071—Warning Definition

<table>
<thead>
<tr>
<th>IMPORTANT SAFETY INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071</td>
</tr>
</tbody>
</table>

SAVE THESE INSTRUCTIONS

<table>
<thead>
<tr>
<th>BEANGRIJKE VEILIGHEIDSINSTRUCTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.</td>
</tr>
</tbody>
</table>

BEWAAR DEZE INSTRUCTIES
<table>
<thead>
<tr>
<th>Language</th>
<th>Important Notice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Varoitus</td>
<td>TÄRKEITÄ TURVALLISUUSOHJEITA</td>
</tr>
<tr>
<td>Attention</td>
<td>IMPORTANTES INFORMATIONS DE SÉCURITÉ</td>
</tr>
<tr>
<td>Warnung</td>
<td>WICHTIGE SICHERHEITSHINWEISE</td>
</tr>
<tr>
<td>Avvertenza</td>
<td>IMPORTANTI ISTRUZIONI SULLA SICUREZZA</td>
</tr>
<tr>
<td>Advarsel</td>
<td>VIKTIGE SIKKERHETSSI instruksjoner</td>
</tr>
</tbody>
</table>

**Varoitus**


**SÄILYTÄ NÄMÄ OHJEET**

**Attention**

Ce symbole d’avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

**Warnung**


BEWAHREN SIE DIESE HINWEISE GUT AUF.

**Avvertenza**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

**Advarsel**

Dette advarselssymbot betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettselen i de oversatte sikkertetsadvarlene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE
INSTRUÇÕES IMPORTANTES DE SEGURANÇA.
Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES.

INSTRUCCIONES IMPORTANTES DE SEGURIDAD
Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

VIKTIGA SÄKERHETSANVISNINGAR

SPARA DESSA ANVISNINGAR.

FONTOS BIZTONSÁGI ELOÍRÁSOK
Az ilyen figyelmezetlen elvek nem vannak meg. Előfordulhat, hogy nagyon veszélyes panasz előfordulhat, ami létrehozhat veszélyt a fizikai egészségügyi terén. Fontos megjegyezni, hogy bármelyik esetben a biztonságos használat tárgyalás és a hibakeresés gyakorlati eljárásokat keresni. A kiadóknotationban szereplő figyelmeztetések fordítása a készülékhöz mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján kereszheli meg.

ORIZZÉ MEG EZEKET AZ UTASÍTÁSOKAT!

Для обеспечения соответствия требованиям по предельным значениям облучения радиочастотами (РЧ) антенны данного устройства должны располагаться на расстоянии не ближе 2 м от пользователей.

Преупреждение

如果电源出现故障或中断，您将无法使用 Voice over IP (VoIP) 服务与紧急呼叫服务。电源恢复之后，您可能需要重新设置或重新配置设备，以便重新获得进入 VoIP 与紧急呼叫服务的权限。在美国，此紧急呼叫号码是 911。您必须知道本国的紧急呼叫号码。

警告

電源障害や停電の場合、ボイス オーバー インピーダンス (VoIP) サービスと緊急呼び出しサービスは機能しません。電源の回復後、VoIP と緊急呼び出しサービスにアクセスするには機器をリセットまたは再設定する必要があります。米国内の緊急呼び出し番号は 911 です。お住まいの地域の緊急呼び出し番号をあらかじめ調べておいてください。

警告
INDEX

<$nopage> HTTP over SSL  703
  see HTTPS  703
<$nopage> IEEE 802.3ad  234
  See EtherChannel  234
<$nopage> PAgP  231
  See EtherChannel  231
<$nopage> Port Aggregation Protocol  231
  See EtherChannel  231
<$nopage> Secure Copy Protocol  647

A

AAA (authentication, authorization, and accounting)  582, 583, 584, 587, 588, 589, 591, 592, 594, 595, 598, 599, 600, 601, 603, 604, 607, 609
  accounting  582, 584, 587, 588, 589, 591, 594, 595, 598, 599, 600, 603, 604, 609
  AV pairs  595
  broadcasting  594, 609
  command type  588
  connection type  589
  enabling  595
  EXEC type  587
  interim records  598
  method lists (example)  582
  monitoring  603
  network type  584
  resource type  591
  suppress records  598, 599
  system type  591
  types  584, 588
  verifying  604
  authorization  583
    network configuration (figure)  583
  server groups  583
  broadcast accounting  594, 609
  method lists  582, 583
    accounting  582
    authorization  583
    resource accounting  592, 600
    configuring  600
  resource failure stop accounting  591, 600
    configuring  600
  server groups  583, 594, 609
  authorization  583

AAA (authentication, authorization, and accounting) (continued)
  server groups (continued)
    broadcast accounting  594, 609
    session MIB  594, 601, 607, 609
      configuration  601
      example  607
      SNMP  594
  aaa accounting resource start-stop group command  600
  aaa accounting resource stop-failure group command  600
  access control entries  742
    See ACEs  742
  access groups  752
    Layer 3  752
  access groups, applying IPv4 ACLs to interfaces  770
  access lists  747, 753
    applying to interfaces  753
    See ACLs  747
  accounting  497, 527, 569
    with RADIUS  569
    with TACACS+  497, 527
  accounting, defined  497
  ACEs  741
    Ethernet  741
    IP  741
  ACL  428, 430, 431, 434
    ACL  428
      IPv4  428
      IP extended  430
      IP standard  428
      IPv4  430
      IPv6  431
    Layer 2 MAC  434
  ACLs  113, 428, 741, 747, 748, 751, 752, 753, 754, 755, 756, 762, 767, 768, 770, 771, 784
    applying  767, 770
      time ranges to  767
      to an interface  770
    classifying traffic for QoS  428
    defined  747
    examples of  428
      extended IPv4  747, 756
      creating  756
      matching criteria  747
    interface  752
ACLs (continued)

IP 747, 748, 753, 762
  implicit deny 762
  implicit masks 748
  matching criteria 747
  undefined 753
IPv4 747, 752, 768, 770
  applying to interfaces 770
  creating 747
  interfaces 752
  matching criteria 747
  numbers 747
  terminal lines, setting on 768
  unsupported features 747
logging messages 754
  matching 753
  monitoring 771
  port 741
QoS 428
  standard IPv4 747, 755
    creating 755
    matching criteria 747
  support in hardware 751
  time ranges to 752
  types supported 741
  unsupported features 747
IPv4 747
activity check 383, 401
  testing 401
  additional references 411
address aliasing 61
address resolution 908
addresses 134, 906, 907, 908, 926
  dynamic 134, 906, 907
    accelerated aging 134
    default aging 134
    defined 906
    learning 907
  MAC, discovering 908
  multicast 134
    STP address management 134
  static 926
    adding and removing 926
aggregate policers 445, 463, 464
aggregate-port learners 245
aging time 146, 180, 919
  accelerated 146, 180
    for MSTP 180
    for STP 146
  MAC address table 919
alternate 126
  port 126
  and ARP 992
  and CDP 992
  and SSH 647
ARP 908
  defined 908
  table 908
    address resolution 908
  attributes 379, 571, 573
    vendor-proprietary 573
    vendor-specific 571
  attributes, RADIUS 571, 573, 577
    vendor-proprietary 573, 577
    vendor-specific 571
  authentication 497, 521, 523, 563, 611
    local mode with AAA 611
  RADIUS 563
    login 563
  TACACS+ 497, 521, 523
    defined 497
    key 521
    login 523
  authentication key 521
  authentication, defined 497
  authoritative time source, described 902
  authorization 497, 525, 568
    with RADIUS 568
    with TACACS+ 497, 525
  authorization, defined 497
  auto-MDIX 28
    configuring 28
    described 28
  auto-MDIX, configuring 28
  automatic creation of 231, 234
  autonegotiation 1006
  mismatches 1006
B

  BackboneFast 199, 213
    described 199
    enabling 213
  backup 126
    port 126
  banners 906, 916, 917
    configuring 916, 917
    login 917
    message-of-the-day login 916
    default configuration 906
  Berkeley r-tools replacement 647
  binding database 804
    address, DHCP server 804
      See DHCP, Cisco IOS server database 804
    binding physical and logical interfaces 230
    bindings 804
      address, Cisco IOS DHCP server 804
      blocking 131
      state 131
default configuration (continued)
  RADIUS 542
  SPAN 328
  SSL 706
  STP 136
  TACACS+ 521
  UDLD 270
default Ethernet VLAN configuration 1092
default gateway 952
default VLAN configuration 1093
defined 279, 289, 497, 704
  Event Service 279
  NameSpace Mapper 279
defining AAA server groups 566
definition 1088
VLAN 1088
deletion 1095
VLAN 1095
described 28, 228, 231, 703, 979, 991, 994, 1127
designated 126
  port 126
  switch 126
detecting communication failure 404
detecting indirect link failures, STP 199
device 132
  root 132
device priority 145, 177
  MSTP 177
  STP 145
devices supported 4
DHCP 799, 807
  enabling 799, 807
  relay agent 807
  server 799
DHCP option 82 801, 808, 815
  displaying 815
  forwarding address, specifying 808
  helper address 808
  overview 801
DHCP server port-based address allocation 816, 818
  default configuration 816
  enabling 816
DHCP snooping 800, 801
  accepting untrusted packets form edge switch 800
  option 82 data insertion 801
  trusted interface 800
  untrusted messages 800
DHCP snooping binding database 804, 805, 811, 816
  adding bindings 816
  binding file 804, 805
  format 805
  location 804
  configuration guidelines 811
  configuring 816
  described 804
  enabling 816
Differentiated Services (Diff-Serv) architecture 416
Differentiated Services Code Point 417
directories 1025, 1026
  changing 1025
  creating 1026
  displaying the working 1025
  removing 1026
disabled 132
  state 132
  disabling 107
  disabling EnergyWise 404
  disabling recovery of 483
disclaimer 1147
displaying 713, 1010
DNIS (Dialed Number Identification Service) 518
  DNIS number 518
  server groups, selecting 518
DNS 906, 915
  default configuration 906
  overview 906
  setting up 915
  domain 377
  Domain Name System 906
  See DNS 906
  domain names 906, 1071
  DNS 906
  DSCP 417
dual-action detection 234
dynamic access ports 1129
  configuring 1129
dynamic addresses 134
  See addresses 134
dynamic port membership described 1127
  reconfirming 1132
  troubleshooting 1134
dynamic port VLAN membership 1127, 1132, 1134
  described 1127
  reconfirming 1131, 1132
  troubleshooting 1134
types of connections 1129
dynamic VLAN assignments 1126

E
  egress expedite queue 421
  egress queue 422, 424
  egress queues 420, 423
  ELIN location 33
  enable 480, 1010
  enable password 482
  enable secret 482
  enable secret password 482
  enabling 105
  enabling all system diagnostics 1017
global leave, IGMP 77

Hello time 146, 179
MSTP 179
STP 146

hosts, limit on dynamic ports 1134
hot-standby ports 247
HTTP secure server 703
HTTPS 703, 704, 707
configuring 707
described 703
self-signed certificate 704

ICMP 737, 992
Host Unreachable message 737
time-exceeded messages 992
trace route and 992
ICMP ping 991, 1007
executing 1007
overview 991
Identifying the RADIUS Server Host: Examples command 575
identifying the server 521
IEEE 802.1Q tagging 1114
IEEE 802.1s 153
See MSTP 153
IEEE 802.3ad, described 234
IGMP 62, 63, 64, 74, 76, 77, 78, 82, 105, 107, 108
configurable leave timer 64, 74
described 64
enabling 74
flooded multicast traffic 76, 77, 78
controlling the length of time 76
disabling on an interface 78
global leave 77
recovering from flood mode 77
join messages 62
leave processing, enabling 105
leaving multicast group 63
queries 62
report suppression 64, 82, 107
described 64
disabling 82, 107
snooping 108
supported versions 62
IGMP filtering 65, 66
default configuration 66
described 65
IGMP groups 87, 88
configuring filtering 88

IGMP groups (continued)
setting the maximum number 87
IGMP Immediate Leave 60, 73
enabling 73
IGMP profile 83, 85
applying 85
configuration mode 83
IGMP report suppression 60
IGMP snooping 59, 61, 62, 64, 65, 66, 67, 80, 100, 101, 102, 108
and address aliasing 61
default configuration 65, 100, 101
definition 61
enabling and disabling 66, 102
global configuration 66
Immediate Leave 64
monitoring 108
querier 59, 80
configuration guidelines 59
configuring 80
supported versions 62
VLAN configuration 67
IGMP throttling 65, 66, 88, 91
configuring 88
default configuration 66
described 65
displaying action 91
IGMP Throttling Action 60
configuration guidelines 60
Immediate Leave, IGMP 64, 105
described 64
enabling 105
interaction with other features 234, 235
interaction with virtual switch interfaces 28
auto-MDIX, configuring 28
Intrusion Detection System 328
See IDS appliances 328
inventory management TLV 33
IP ACLs 749
named 749
IP addresses 908
discovering 908
IP addresses and subnets 992
IP precedence 417
IP traceroute 992, 1008
executing 1008
overview 992
IP unicast routing 952
default 952
gateways 952
IPv4 ACLs 752, 755, 756, 759, 770
applying to interfaces 770
extended, creating 756
interfaces 752
named 759
standard, creating 755
IPv6 97, 113, 784
ACL 113, 784
SDM templates 97

J
join messages, IGMP 62

K
keepalive messages 126
key 521

L
LACP 228, 235, 241, 247, 248, 250
hot-standby ports 247
interaction with other features 235
min links 250
modes 235
port priority 248
system priority 247
Layer 2 EtherChannel configuration guidelines 239
Layer 2 interface modes 1106
Layer 2 interfaces 241
Layer 2 traceroute 991, 992
and ARP 992
and CDP 992
broadcast traffic described 991
IP addresses and subnets 992
MAC addresses and VLANS 992
multicast traffic 992
multiple devices on a port 992
unicast traffic 991
usage guidelines 992
Layer 3 packets, classification methods 417
learn method and priority configuration 245
leave processing, enabling 105
limiting the services to the user 525, 568
Link Failure, detecting unidirectional listening 131
state 131
LLDP 31, 33, 34, 36
configuring 33
default configuration 33
enabling 34
overview 31
switch stack considerations 31
transmission timer and holdtime, setting 36
LLDP-MED 32, 38
configuring 38
TLVs 38
overview 32
supported TLVs 32
load sharing 1108, 1116, 1120
trunk ports 1108
local mode with AAA 611
location TLV 33
logging into 491
logging messages, ACL 754
logical interfaces, described 230
login 523, 563
login authentication with RADIUS 563
with TACACS+ 523
login banners 906

M
MAC address-table move update 261, 263, 264
configuration guidelines 263
configuring 263
description 261
obtain and process messages 264
MAC addresses 907, 908, 919, 926
aging time 919
and VLAN association 907
building the address table 907
default configuration 907
discovering 908
dynamic 907
learning 907
static 926
characteristics of 926
MAC addresses and VLANS 992
MAC extended access lists 746
applying to Layer 2 interfaces 746
MAC/PHY configuration status TLV 31
management address TLV 31
mapping table 425
default configuration 425
mapping tables for QoS 419
described 419
marking 440, 445, 463, 464
action in policy map 440
action with aggregate policers 445, 463, 464
maximum aging time 147, 181
MSTP 181
STP 147
maximum hop count, MSTP 182
memory allocation 422
messages, to users through banners 906
method lists 582, 583
AAA 582, 583
accounting 582
authorization 583
MIB support 411
min links 250
mirroring traffic for analysis 328
mismatches 1006
mismatches, autonegotiation 1006
MLD Messages 98
MLD Queries 98
MLD Reports 99
MLD Snooping 97
MLDv1 Done message 100
modes 232, 235
monitoring 91, 108, 458, 713, 771, 1007, 1084, 1144
access groups 771
IGMP 108
snooping 108
IPv4 ACL configuration 771
multicast router interfaces 91
SFP status 1007
voice VLAN 1144
VTP 1084
monitoring commands 403
monitoring status of 1007
MST mode 1108
MSTP 135, 151, 152, 153, 154, 155, 156, 157, 158, 159, 161, 166, 170, 172, 173, 174, 176, 177, 179, 180, 181, 182, 183, 184, 185, 192, 196, 197, 201, 202, 203, 206, 208, 209, 214, 215, 216
boundary ports 151, 159
coloration guidelines 151
described 159
BPDU filtering 197, 209
described 197
enabling 209
BPDU guard 196, 208
described 196
enabling 208
CIST regional root 156, 157
CIST root 157
CIST, described 155
coloration guidelines 153
coloring 170, 172, 173, 174, 176, 177, 179, 180, 181, 182, 183, 184
device priority 177
forward-delay time 180
hello time 179
link type for rapid convergence 183
maximum aging time 181
maximum hop count 182
MST region 170
neighbor type 184
path cost 176
port priority 174
root device 172
secondary root device 173
CST 156
operations between regions 156
default configuration 166
displaying status 192
enabling the mode 170
EtherChannel guard 201, 214
described 201
MSTP (continued)
EtherChannel guard (continued)
enabling 214
extended system ID 154, 173
effects on root device 154
effects on secondary root device 173unexpected behavior 154
IEEE 802.1s 156, 159
implementation 159
port role naming change 159
terminology 156
instances supported 135
interface state, blocking to forwarding 196
interoperability and compatibility among modes 135, 152
interoperability with IEEE 802.1D 161, 185
described 161
restarting migration process 185
IST 156
operations within a region 156
loop guard 203, 216
described 203
enabling 216
mapping VLANs to MST instance 170
MST region 154, 155, 158, 170
CIST 155
coloring 170
described 154
hop-count mechanism 158
IST 155
supported spanning-tree instances 155
PortFast 196, 206
described 196
enabling 206
preventing root switch selection 202
root device 154
coloring 154
effects of extended system ID 154unexpected behavior 154
root guard 202, 215
described 202
enabling 215
shutdown Port Fast-enabled port 196
status, displaying 192
MTU 45
system 45
Multicast Client Aging Robustness 99
multicast groups 62, 63, 72, 103
joining 62
leaving 63
static joins 72, 103
Multicast Router Discovery 99
multicast router interfaces, monitoring 91
multicast router ports, adding 70
multicast traffic 992
multiple devices on a port 992
N
NameSpace Mapper 279
native VLAN 1114
network 376
Network Load Sharing 1108
STP path cost 1108
STP priorities 1108
network policy TLV 32
nonhierarchical policy maps 440
configuring 440
normal-range 1090
VLAN configuration guidelines 1090
NTP 902, 904
associations 904
defined 904
overview 902
time 904
services 904
numbering of 230

O
OBFL 994, 1010
configuring 1010
described 994
displaying 1010
on Layer 2 interfaces 241
on-board failure logging 994
online diagnostics 979
defined 979
overview 979
operation of 498, 541
overview 475, 479, 497, 541, 979, 991, 992

P
PaGP 228
PAgP 231, 232, 234, 241, 245
aggregate-port learners 245
described 231
interaction with other features 234
interaction with virtual switches 234
learn method and priority configuration 245
modes 232
with dual-action detection 234
partitioned 1005
password 1072
password and privilege level 478
password recovery disable considerations 483
passwords 475, 478, 480, 482, 483, 485, 486, 989
default configuration 478
disabling recovery of 483
encrypting 482
overview 475

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
PVST mode 1108
PVST+ 134, 135, 136
described 134
IEEE 802.1Q trunking interoperability 136
instances supported 135

451, 452, 454, 455, 457, 463, 464
class maps 436, 438
configuring 436, 438
configuring 428, 440, 445, 447, 463, 464
aggregate policers 445, 463, 464
egress queue characteristics 447
IP standard ACLs 428
policy maps on physical ports 440
default configuration 424
egress queues 423, 449, 451, 452, 454
configuring shaped weights for SRR 452
configuring shared weights for SRR 454
displaying the threshold map 451
mapping DSCP or CoS values 449
WTD, described 423
enabling globally 425
enabling VLAN-based on physical ports 426
limiting bandwidth on egress interface 457
mapping tables 419
types of 419
marked-down actions 443
policers 443
configuring 443
queues 420, 423, 447, 455
configuring egress characteristics 447
high priority (expedite) 423, 455
location of 420
QoS policy 428
queries 382, 397
queries, IGMP 62
querying 409, 410
domains 409
keywords 410
name attribute 409
set power levels 410
queueing 420

RADIUS (continued)
configuring (continued)
authorization 568
communication, global 562
default configuration 542
defining AAA server groups 566
limiting the services to the user 568
login 563
operation of 541
overview 541
suggested network environments 541
tracking services accessed by user 569
rapid convergence 162
Rapid Spanning Tree Protocol 153
See RSTP 153
reconfirmation interval, changing 1132
reconfirmation interval, VMPS, changing 1132
reconfirming 1131, 1132
reconfirming dynamic VLAN membership 1131
reconfirming membership 1131
recovery of 989
recurrences 380, 381, 394
configuring 28, 241, 388, 391, 392, 394, 400, 521, 523, 525, 527, 562,
563, 568, 569, 648, 707, 710, 711, 1129
day of month 381
day of week 381
redirecting error message output 1009
redundancy 133, 228
EtherChannel 228
STP 133
backbone 133
redundant links and UplinkFast 210, 212
reference 160
Remote Authentication Dial-In User Service 540
See RADIUS 540
report suppression 107
disabling 107
report suppression, IGMP 64, 82, 107
described 64
disabling 82, 107
restricting access 475, 497, 540
overview 475
RADIUS 540
TACACS+ 497
restrictions 60, 125, 152, 195, 277, 1066, 1126, 1140
Configuration Engine 277
IGMP snooping 60
MSTP 152
Optional Spanning-Tree Features 195
STP 125
voice VLANs 1140
VTP 1066
retry count, changing 1133
retry count, VMPS, changing 1133
RFC 61, 902
1112, IP multicast and IGMP 61

INDEX
RFC (continued)
   1305, NTP 902
   role 126
   port 126
root 126, 127
   port 126, 127
 switch 126, 127
root device 139, 172
MSTP 172
STP 139
RSTP 161, 162, 163, 164, 165, 183, 185
   active topology 162
 BPDU 164, 165
   format 164
   processing 165
   designated port, defined 161
   designated switch, defined 161
   interoperability with IEEE 802.1D 161, 165, 185
      described 161
      restarting migration process 185
      topology changes 165
      overview 161
 port roles 161, 163
      described 161
      synchronized 163
   rapid convergence 162, 183
      described 162
      edge ports and Port Fast 162
      point-to-point links 162, 183
 root ports 162
root port, defined 161
RTC 902
   benefits 902
   defined 902

S
   scheduling 420
SCP 647, 648
   and SSH 647
      configuring 648
 SDM templates 97
 secure HTTP client 710, 713
      configuring 710
      displaying 713
 secure HTTP server 707, 713
      configuring 707
      displaying 713
Secure Shell 646
Secure Shell Version 2 679, 680, 689
      monitoring and maintaining 680
      verifying using the show ip ssh command 679
SecureOn 384
   security 380
   security and identification 1007
See also IP traceroute 992
See EtherChannel 231, 234
see HTTPS 703
See RADIUS 540
See SCP 647
See TACACS+<SNAP> 497
 self-signed certificate 704
 server groups 583
       AAA, authorization 583
       server groups, AAA 594, 609
       broadcast accounting 594, 609
       service-provider network, MSTP and RSTP 153
       services 279
       networking 279
 setting 480, 482, 485, 486
       enable 480
       enable secret 482
       Telnet 485
       with usernames 486
 setting a command with 488
 setting a password 485
 Setting a Telnet Password for a Terminal Line: Example command 492
 Setting or Changing a Static Enable Password: Example command 492
 setting packet forwarding 1009
 Setting the Privilege Level for a Command: Example command 493
 SFP security and identification 1007
 SFPs 1007
      monitoring status of 1007
      security and identification 1007
      status, displaying 1007
 shaped mode 423
 shared mode 423
 show access-lists hw-summary command 752
 show forward command 1009
 show platform forward command 1009
 Simple Network Management Protocol (SNMP) 289
 single-switch EtherChannel 229
 SNMP 920, 922, 924
      traps 920, 922, 924
      enabling MAC address notification 920, 922, 924
 SPI 108
 SPAN 328, 329, 331
      configuration guidelines 329
      default configuration 328
      overview 328
      sessions 329, 331
      creating 329
      removing destination (monitoring) ports 329
      specifying monitored ports 329
      with ingress traffic enabled 331
 Spanning Tree 130
      states 130
 spanning-tree 126
      port priority 126
SSH 646, 647
      encryption methods 647
### SSH (continued)
- User authentication methods, supported 647
- Server 650
- SSL 647, 706, 707, 710, 713
  - Configuration guidelines 647, 706
  - Configuring a secure HTTP client 710
  - Configuring a secure HTTP server 707
  - Monitoring 713
- Stack changes, effects on 238
- Cross-stack EtherChannel 238
- Stacks, 127, 135
  - MSTP instances supported 135
  - STP 127
    - Bridge ID 127
    - Switch 135
- Stacks, switch 905, 1005
  - Partitioned 1005
  - System prompt consideration 905
- Static addresses 907
- Static-access ports 1097
- Status, displaying 1007
- STP 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 141, 142, 143, 145, 146, 147, 148, 149, 152, 197, 198, 199, 201, 210, 212, 213, 214
  - Accelerating root port selection 198
  - BackboneFast 199, 213
    - Described 199
    - Enabling 213
  - BPDU message exchange 127
    - Configuring 137, 139, 141, 142, 143, 145, 146, 147, 148
      - Device priority 145
      - Forward-delay time 146
      - Hello time 146
      - Maximum aging time 147
      - Path cost 143
      - Port priority 142
      - Root device 139
      - Secondary root device 141
      - Spanning-tree mode 137
      - Transmit hold-count 148
    - Default configuration 136
    - Designated, defined 127
      - Switch 127
    - Designated port, defined 127
    - Detecting indirect link failures 199
    - Disabling 138
    - Displaying status 149
    - EtherChannel guard 201, 214
      - Described 201
      - Enabling 214
    - Extended system ID 125, 128, 139, 141
      - Effects on root device 139
      - Effects on the secondary root device 141
      - Overview 128
- STP (continued)
  - Extended system ID (continued)
    - Unexpected behavior 125
  - IEEE 802.1D and bridge ID 128
  - IEEE 802.1D and multicast addresses 134
  - IEEE 802.1t and VLAN identifier 128
  - Instances supported 135
  - Interface states 130, 131, 132
    - Blocking 131
    - Disabled 132
    - Forwarding 131, 132
    - Learning 131
    - Listening 131
  - Interoperability and compatibility among modes 135, 152
  - Keepalive messages 126
  - Limitations with IEEE 802.1Q trunks 135
  - Modes supported 134
  - Overview 126
  - Protocols supported 134
  - Redundant connectivity 133
  - Root 125, 127
    - Election 127
    - Switch 125, 127
    - Unexpected behavior 125
  - Root device 128, 129, 139
    - Configuring 129
    - Effects of extended system ID 128, 139
  - Root port, defined 127
  - Status, displaying 149
  - UplinkFast 197, 210, 212
    - Described 197
    - Disabling 212
    - Enabling 210
  - VLAN-bridge 136
  - STP path cost 1120
  - STP port priorities 1116
  - Stratum, NTP 903
  - Subnetwork Access Protocol (SNAP) 289
  - Suggested network environments 541
  - Summer time 910
  - Supported watts per port 4
  - Switch Access 492
    - Displaying 492
  - Switch stack 1010
  - System 45
    - System capabilities TLV 31
    - System clock 901, 908, 909, 910
      - Configuring 908, 909, 910
        - Daylight saving time 910
        - Manually 908
        - Summer time 910
        - Time zones 909
      - Overview 901
    - System description TLV 31
    - System name 905, 913
      - Default configuration 905
system name (continued) 913
  manual configuration 913
system name TLV 31
system priority 247
system prompt, default setting 905

T

TACACS+ 497, 498, 499, 506, 518, 520, 521, 523, 525, 527, 532
  accounting, defined 497
  authorization 520
  authentication, defined 497
AV pairs 499, 506
  accounting 506
  configuring 518, 520, 521, 523, 525, 527
  authorization 520
  authentication key 521
  authorization 525
  DNIS, server group selection 518
  login authentication 523
  server groups 518
  DNIS selection 518
  default configuration 521
  defined 497
  displaying 532
  identifying the server 521
  key 521
  limiting the services to the user 525
  login 523
  operation of 498
  overview 497
  server groups 518
  DNIS selection 518
  tracking services accessed by user 527
tar files 1028
  creating 1028
  displaying the contents of 1028
  extracting 1028
  technical assistance 411
Telnet 485
  setting a password 485
temporary self-signed certificate 704
Terminal Access Controller Access Control System Plus 497
  See TACACS+<snopage>  497
terminal lines, setting a password 485
time 901
  See NTP and system clock 901
  time format 381
time ranges in ACLs 752, 767
time zone 381
time zones 909
time-exceeded messages 992
time-range command 752
tLVs 31
  defined 31
Token Rings 1077
Topology Change Notification Processing 100
tcrouter and 992
tcrouter command 992
  See also IP tcrouter 992
tcrouter, Layer 2 991, 992
  and ARP 992
  and CDP 992
  broadcast traffic 991
described 991
  IP addresses and subnets 992
  MAC addresses and VLANs 992
  multicast traffic 992
  multiple devices on a port 992
  unicast traffic 991
  usage guidelines 992
tracking services accessed by user 527, 569
  traffic 742
    fragmented 742
traps 920, 922, 924
  configuring MAC address notification 920, 922, 924
  enabling 920, 922, 924
troubleshooting 991, 992, 994, 1007, 1009, 1134
  setting packet forwarding 1009
  SFP security and identification 1007
  show forward command 1009
  with debug commands 994
  with ping 991
  with tcrouter 992
Troubleshooting Examples command 1015
  trunk 1109, 1111
    configuration 1109
  trunk port 1109
  trunking 1106
  trunking modes 1106
  trunks 1107
    allowed VLANs 1107
  trustpoints, CA 704
twisted-pair, detecting unidirectional links 268
types of connections 1129

U

UDLD 267, 268, 269, 270, 272
  aggressive 268
  aggressive mode 270
  message time 270
  default configuration 270
disable 272
  per interface 272
echoing detection mechanism 269
enabling 270, 272
globally 270

Software Configuration Guide, Cisco IOS Release 15.2(5)EX (Cisco Digital Building Switches)
software configuration guide, cisco ios release 15.2(5)ex (cisco digital building switches)