Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)

First Published: 2017-08-08
Last Modified: 2018-12-18
CONTENTS

PREFACE

Preface  lv
  Document Conventions  lv
  Obtaining Documentation and Submitting a Service Request  lvii

CHAPTER 1

Using the Command-Line Interface  1
  Information About Using the Command-Line Interface  1
  Command Modes  1
  Understanding Abbreviated Commands  3
  No and Default Forms of Commands  3
  CLI Error Messages  3
  Configuration Logging  4
  Using the Help System  4
  How to Use the CLI to Configure Features  5
  Configuring the Command History  5
    Changing the Command History Buffer Size  5
    Recalling Commands  6
    Disabling the Command History Feature  6
  Enabling and Disabling Editing Features  7
    Editing Commands Through Keystrokes  7
    Editing Command Lines That Wrap  8
  Searching and Filtering Output of show and more Commands  9
  Accessing the CLI Through a Console Connection or Through Telnet  10
  Accessing the CLI through Bluetooth  10

PART I

Interface and Hardware  13
CHAPTER 2  Configuring Interface Characteristics 15

Finding Feature Information 15

Information About Configuring Interface Characteristics 15

Interface Types 15

Port-Based VLANs 15

Switch Ports 16

Routed Ports 17

Switch Virtual Interfaces 17

EtherChannel Port Groups 18

Power over Ethernet Ports 18

Using the Switch USB Ports 18

USB Mini-Type B Console Port 18

USB Type A Ports 19

Interface Connections 19

Interface Configuration Mode 19

Default Ethernet Interface Configuration 20

Interface Speed and Duplex Mode 21

Speed and Duplex Configuration Guidelines 21

IEEE 802.3x Flow Control 22

How to Configure Interface Characteristics 23

Configuring Interfaces 23

Adding a Description for an Interface 24

Configuring a Range of Interfaces 25

Configuring and Using Interface Range Macros 26

Configuring Ethernet Interfaces 28

Setting the Interface Speed and Duplex Parameters 28

Configuring IEEE 802.3x Flow Control 29

Shutting Down and Restarting the Interface 30

Configuring the Console Media Type 32

Configuring the USB Inactivity Timeout 33

Monitoring Interface Characteristics 34

Monitoring Interface Status 34

Clearing and Resetting Interfaces and Counters 35
## Finding Feature Information

Restrictions for EEE

Information About EEE

EEE Overview

Default EEE Configuration

How to Configure EEE

Enabling or Disabling EEE

Monitoring EEE

Configuration Examples for Configuring EEE

Additional References

Feature Information for Configuring EEE

### PART II

**IP Multicast Snooping**

### CHAPTER 8

**Configuring IGMP Snooping**

Finding Feature Information

Prerequisites for Configuring IGMP Snooping

Prerequisites for IGMP Snooping

Restrictions for Configuring IGMP Snooping

Restrictions for IGMP Snooping

Information About IGMP Snooping

IGMP Snooping

IGMP Versions

Joining a Multicast Group

Leaving a Multicast Group

Immediate Leave

IGMP Configurable-Leave Timer

IGMP Report Suppression

Default IGMP Snooping Configuration

IGMP Filtering and Throttling

Default IGMP Filtering and Throttling Configuration

How to Configure IGMP Snooping

Enabling or Disabling IGMP Snooping on a Switch

Enabling or Disabling IGMP Snooping on a VLAN Interface
Configuring IPv6 ACL 147
Finding Feature Information 147
Information About Configuring IPv6 ACLs 147
Understanding IPv6 ACLs 147
Supported ACL Features 148
IPv6 ACL Limitations 148
Configuring IPv6 ACLs 148
Default IPv6 ACL Configuration 149
Interaction with Other Features and Switches 149
Creating IPv6 ACL 149
Applying an IPv6 ACL to an Interface 153
Displaying IPv6 ACLs 153
Configuration Examples for IPv6 ACL 154
Example: Creating an IPv6 ACL 154
Example: Displaying IPv6 ACLs 154

PART IV
Layer 2 157

CHAPTER 12
Configuring Spanning Tree Protocol 159
Finding Feature Information 159
Restrictions for STP 159
Information About Spanning Tree Protocol 160
Spanning Tree Protocol 160
Spanning-Tree Topology and BPDUs 161
Bridge ID, Device Priority, and Extended System ID 162
Port Priority Versus Path Cost 163
Spanning-Tree Interface States 163
How a Switch or Port Becomes the Root Switch or Root Port 166
Spanning Tree and Redundant Connectivity 166
Contents

Enabling PVST+ Simulation on a Port 221

Examples 222

Examples: PVST+ Simulation 222

Examples: Detecting Unidirectional Link Failure 226

Monitoring MST Configuration and Status 226

Feature Information for MSTP 227

CHAPTER 14 Configuring Optional Spanning-Tree Features 229

Finding Feature Information 229

Restriction for Optional Spanning-Tree Features 229

Information About Optional Spanning-Tree Features 230

PortFast 230

BPDU Guard 230

BPDU Filtering 231

UplinkFast 231

BackboneFast 233

EtherChannel Guard 235

Root Guard 236

Loop Guard 237

STP PortFast Port Types 237

Bridge Assurance 238

How to Configure Optional Spanning-Tree Features 240

Enabling PortFast 240

Enabling BPDU Guard 242

Enabling BPDU Filtering 243

Enabling UplinkFast for Use with Redundant Links 244

Disabling UplinkFast 246

Enabling BackboneFast 247

Enabling EtherChannel Guard 248

Enabling Root Guard 249

Enabling Loop Guard 250

Enabling PortFast Port Types 251

Configuring the Default Port State Globally 252

Configuring PortFast Edge on a Specified Interface 253
Contents

CHAPTER 15 Configuring Resilient Ethernet Protocol 261
Finding Feature Information 261
Overview of Resilient Ethernet Protocol 261
  Link Integrity 263
  Fast Convergence 264
  VLAN Load Balancing 264
  Spanning Tree Interaction 265
  REP Ports 266
How to Configure Resilient Ethernet Protocol 266
  Default REP Configuration 266
  REP Configuration Guidelines 266
  Configuring REP Administrative VLAN 268
  Configuring a REP Interface 269
  Setting Manual Preemption for VLAN Load Balancing 273
  Configuring SNMP Traps for REP 274
Monitoring Resilient Ethernet Protocol Configuration 274
Configuration Examples for Resilient Ethernet Protocol 276
  Example: Configuring the REP Administrative VLAN 276
  Example: Configuring a REP Interface 276
Additional References for REP 277
Feature Information for Resilient Ethernet Protocol 278

CHAPTER 16 Configuring EtherChannels 279
Finding Feature Information 279
Restrictions for EtherChannels 279
### CHAPTER 17

**Configuring Link-State Tracking**

- Finding Feature Information
- Restrictions for Configuring Link-State Tracking
- Understanding Link-State Tracking
- How to Configure Link-State Tracking
- Monitoring Link-State Tracking
- Configuring Link-State Tracking: Example
- Feature Information for Link-State Tracking

### CHAPTER 18

**Configuring UniDirectional Link Detection**

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

### PART V

**Network Management**

### CHAPTER 19

**Configuring Cisco IOS Configuration Engine**

- Prerequisites for Configuring the Configuration Engine
Restrictions for Configuring the Configuration Engine 323
Information About Configuring the Configuration Engine 324
Cisco Configuration Engine Software 324
Configuration Service 325
Event Service 325
NameSpace Mapper 326
Cisco Networking Services IDs and Device Hostnames 326
ConfigID 326
DeviceID 326
Hostname and DeviceID 327
Hostname, DeviceID, and ConfigID 327
Automated CNS Configuration 327
How to Configure the Configuration Engine 328
Enabling the CNS Event Agent 328
Refreshing DeviceIDs 330
Monitoring CNS Configurations 332
Additional References 333
Feature History and Information for the Configuration Engine 334

CHAPTER 20
Configuring the Cisco Discovery Protocol 335
Finding Feature Information 335
Information About CDP 335
Cisco Discovery Protocol Overview 335
Default Cisco Discovery Protocol Configuration 336
How to Configure CDP 336
Configuring Cisco Discovery Protocol Characteristics 336
Disabling Cisco Discovery Protocol 338
Enabling Cisco Discovery Protocol 340
Disabling Cisco Discovery Protocol on an Interface 341
Enabling Cisco Discovery Protocol on an Interface 343
Monitoring and Maintaining Cisco Discovery Protocol 344
Additional References 345
Feature History and Information for Cisco Discovery Protocol 346
How to Configure SPAN 373
  Creating a Local SPAN Session 373
  Creating a Local SPAN Session and Configuring Incoming Traffic 375
Monitoring SPAN Operations 377
SPAN Configuration Examples 377
  Example: Configuring Local SPAN 377
Additional References 378
Feature History and Information for SPAN 379

PART VI  QoS 381

CHAPTER 23 Configuring QoS 383
  Finding Feature Information 383
  Prerequisites for QoS 383
    QoS ACL Guidelines 383
    Policing Guidelines 384
    General QoS Guidelines 384
  Restrictions for QoS 384
  Information About QoS 385
  QoS Implementation 385
    Layer 2 Frame Prioritization Bits 386
    Layer 3 Packet Prioritization Bits 386
    End-to-End QoS Solution Using Classification 386
  QoS Basic Model 387
    Actions at Ingress Port 387
    Actions at Egress Port 388
    Classification Overview 388
  Policing and Marking Overview 392
  Queueing and Scheduling Overview 393
  Queueing and Scheduling on Egress Queues 395
  Packet Modification 397
  Standard QoS Default Configuration 398
    Default Egress Queue Configuration 398
    Default Mapping Table Configuration 399
How to Configure QoS 399

Enabling QoS Globally 399

Configuring Classification Using Port Trust States 400

   Configuring the Trust State on Ports Within the QoS Domain 400

   Configuring the CoS Value for an Interface 402

   Configuring a Trusted Boundary to Ensure Port Security 404

   Enabling DSCP Transparency Mode 406

   Configuring the DSCP Trust State on a Port Bordering Another QoS Domain 408

Configuring a QoS Policy 410

   Classifying Traffic by Using ACLs 410

   Classifying Traffic by Using Class Maps 417

   Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps 419

Configuring Egress Queue Characteristics 423

   Configuration Guidelines 423

   Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID 423

   Configuring SRR Shaped Weights on Egress Queues 425

   Configuring SRR Shared Weights on Egress Queues 427

   Configuring the Egress Expedite Queue 428

   Limiting the Bandwidth on an Egress Interface 430

Monitoring Standard QoS 431

Configuration Examples for QoS 432

   Example: Configuring Port to the DSCP-Trusted State and Modifying the DSCP-to-DSCP-Mutation
   Map 432

   Examples: Classifying Traffic by Using ACLs 432

   Examples: Classifying Traffic by Using Class Maps 433

   Examples: Classifying, Policing, and Marking Traffic on Physical Ports Using Policy Maps 434

   Examples: Configuring DSCP-to-DSCP Mutation Maps 435

   Examples: Configuring Egress Queue Characteristics 436

Where to Go Next 437

Feature History and Information for QoS 437

CHAPTER 24

Configuring AutoQoS 439

   Finding Feature Information 439

   Prerequisites for Auto-QoS 439
Restrictions for Auto-QoS 440
Information about Configuring Auto-QoS 440
  Auto-QoS Overview 440
  Auto-QoS Compact Overview 441
Generated Auto-QoS Configuration 441
  VoIP Device Specifics 441
  Enhanced Auto-QoS for Video, Trust, and Classification 442
  Auto-QoS Configuration Migration 442
Auto-QoS Configuration Guidelines 443
  Auto-QoS VoIP Considerations 443
  Auto-QoS Enhanced Considerations 443
Effects of Auto-QoS on Running Configuration 443
Effects of Auto-Qos Compact on Running Configuration 444
How to Configure Auto-QoS 444
  Configuring Auto-QoS 444
    Enabling Auto-QoS 444
    Enabling Auto-Qos Compact 446
    Troubleshooting Auto-QoS 447
Monitoring Auto-QoS 448
Configuration Examples for Auto-Qos 449
  Examples: Global Auto-QoS Configuration 449
  Examples: Auto-QoS Generated Configuration For Enhanced Video, Trust, and Classify Devices 450
    auto qos global compact 452
Where to Go Next for Auto-QoS 453
Additional References for Auto-QoS 453
Feature History and Information for Auto-QoS 454

PART VII  Routing 455

CHAPTER 25  Configuring IP Unicast Routing 457
  Finding Feature Information 457
  Information About Configuring IP Unicast Routing 457
  Information About IP Routing 458
Types of Routing 458
Static Unicast Routes 458
Default Routes and Networks 459
Routing Information Protocol 460
Summary Addresses and Split Horizon 460
Configuring IP Unicast Routing 460
Enabling IP Unicast Routing 461
Example: Enabling IP Unicast Routing 462
Assigning IP Addresses to SVIs 462
Example: Assigning IP Addresses to SVIs 463
Configuring Static Unicast Routes 465
Example: Configuring Static Unicast Routes 465
Configuring Default Routes and Networks 465
How to Configure RIP 466
Default RIP Configuration 466
Configuring Basic RIP Parameters 467
Configuring RIP Authentication 468
Configuring Summary Addresses and Split Horizon 470
Configuring Split Horizon 471
Example: Configuring Summary Addresses and Split Horizon 472
Example: Displaying Current Status of Routing Table 472
Monitoring and Maintaining the IP Network 473

PART VIII  Security 475

CHAPTER 26  Security Features Overview 477
Security Features Overview 477
Feature Information for Security Features 480

CHAPTER 27  Preventing Unauthorized Access 481
Finding Feature Information 481
Preventing Unauthorized Access 481

CHAPTER 28  Controlling Switch Access with Passwords and Privilege Levels 483
Method List  502
TACACS AV Pairs  503
  TACACS Authentication and Authorization AV Pairs  503
  TACACS Accounting AV Pairs  510
TACACS+ Configuration Options  522
TACACS+ Login Authentication  522
TACACS+ Authorization for Privileged EXEC Access and Network Services  523
TACACS+ Authentication  523
TACACS+ Authorization  523
TACACS+ Accounting  523
Default TACACS+ Configuration  523
How to Configure TACACS+  523
  Identifying the TACACS+ Server Host and Setting the Authentication Key  523
  Configuring TACACS+ Login Authentication  525
  Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services  528
Starting TACACS+ Accounting  529
Establishing a Session with a Router if the AAA Server is Unreachable  530
Establishing a Session with a Router if the AAA Server is Unreachable  531
Configuring Per VRF on a TACACS Server  531
Monitoring TACACS+  533
Configuration Examples for TACACS+  533
  Example: TACACS Authorization  533
  Example: TACACS Accounting  534
  Example: TACACS Authentication  534
  Example: Configuring Per VRF for TACACS Servers  536
Additional References for TACACS+  537
Feature Information for TACACS+  538

CHAPTER 30
Configuring RADIUS  539
Finding Feature Information  539
Prerequisites for Configuring RADIUS  539
Restrictions for Configuring RADIUS  540
Information about RADIUS  540
  RADIUS and Switch Access  540
Chapter 31: Configuring Accounting

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
  VRNS 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 596
  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 599
  Configuring AAA Resource Accounting for Start-Stop Records 600
  Configuring AAA Broadcast Accounting 600
Enabling Configurable MAB Username and Password 622
Configuration Examples for MAC Authentication Bypass 623
Example: MAC Authentication Bypass Configuration 623
Example: Enabling Configurable MAB Username and Password 623
Additional References for MAC Authentication Bypass 623
Feature Information for MAC Authentication Bypass 624

Password Strength and Management for Common Criteria 625
Finding Feature Information 625
Restrictions for Password Strength and Management for Common Criteria 626
Information About Password Strength and Management for Common Criteria 626
Password Composition Policy 626
Password Length Policy 626
Password Lifetime Policy 626
Password Expiry Policy 626
Password Change Policy 627
User Reauthentication Policy 627
Support for Framed (Noninteractive) Session 627
How to Configure Password Strength and Management for Common Criteria 628
Configuring the Password Security Policy 628
Verifying the Common Criteria Policy 630
Configuration Examples for Password Strength and Management for Common Criteria 631
Example: Password Strength and Management for Common Criteria 631
Additional References for Password Strength and Management for Common Criteria 631
Feature Information for Password Strength and Management for Common Criteria 632

AAA-SERVER-MIB Set Operation 633
Finding Feature Information 633
Prerequisites for AAA-SERVER-MIB Set Operation 633
Restrictions for AAA-SERVER-MIB Set Operation 634
Information About AAA-SERVER-MIB Set Operation 634
CISCO-AAA-SERVER-MIB 634
CISCO-AAA-SERVER-MIB Set Operation 634
How to Configure AAA-SERVER-MIB Set Operation 634
Configuring AAA-SERVER-MIB Set Operations 634
Verifying SNMP Values 634
Configuration Examples for AAA-SERVER-MIB Set Operation 635
  RADIUS Server Configuration and Server Statistics Example 635
Additional References for AAA-SERVER-MIB Set Operation 637
Feature Information for AAA-SERVER-MIB Set Operation 638

CHAPTER 36

Configuring Secure Shell 639
  Finding Feature Information 639
  Prerequisites for Configuring Secure Shell 639
  Restrictions for Configuring Secure Shell 640
  Information About Configuring Secure Shell 640
    SSH and Switch Access 640
    SSH Servers, Integrated Clients, and Supported Versions 641
    RSA Authentication Support 641
    SSL Configuration Guidelines 641
    Secure Copy Protocol Overview 641
    Secure Copy Protocol 642
    How Secure Copy Works 642
    Reverse Telnet 642
    Reverse SSH 643
  How to Configure Secure Shell 643
    Setting Up the Switch to Run SSH 643
    Configuring the SSH Server 644
    Troubleshooting Tips 646
    Configuring Reverse SSH for Console Access 647
    Configuring Reverse SSH for Modem Access 649
    Troubleshooting Reverse SSH on the Client 650
    Troubleshooting Reverse SSH on the Server 651
    Monitoring the SSH Configuration and Status 652
    Configuring Secure Copy 652
  Configuration Examples for Secure Shell 654
    Example: Secure Copy Configuration Using Local Authentication 654
    Example: SCP Server-Side Configuration Using Network-Based Authentication 654
CHAPTER 37 Secure Shell Version 2 Support 657
Finding Feature Information 657
Information About Secure Shell Version 2 Support 657
Secure Shell Version 2 657
Secure Shell Version 2 Enhancements for RSA Keys 658
SNMP Trap Generation 659
SSH Keyboard Interactive Authentication 660
How to Configure Secure Shell Version 2 Support 660
Configuring a Device for SSH Version 2 Using a Hostname and Domain Name 660
Configuring a Device for SSH Version 2 Using RSA Key Pairs 661
Configuring the Cisco SSH Server to Perform RSA-Based User Authentication 663
Configuring the Cisco IOS SSH Client to Perform RSA-Based Server Authentication 664
Starting an Encrypted Session with a Remote Device 667
Enabling Secure Copy Protocol on the SSH Server 667
Verifying the Status of the Secure Shell Connection 669
Verifying the Secure Shell Status 670
Monitoring and Maintaining Secure Shell Version 2 672
Configuration Examples for Secure Shell Version 2 Support 675
Example: Configuring Secure Shell Version 2 675
Example: Starting an Encrypted Session with a Remote Device 675
Example: Configuring Server-Side SCP 675
Example: Setting an SNMP Trap 675
Examples: SSH Keyboard Interactive Authentication 676
Example: Enabling Client-Side Debugs 676
Example: Enabling ChPass with a Blank Password Change 677
Example: Enabling ChPass and Changing the Password on First Login 677
Example: Enabling ChPass and Expiring the Password After Three Logins 677
Example: SNMP Debugging 678
### CHAPTER 40

**Certification Authority Interoperability**

- Finding Feature Information
- Prerequisites For Certification Authority
- Restrictions for Certification Authority
- Information About Certification Authority
  - CA Supported Standards
  - Purpose of CAs
  - Registration Authorities
- How to Configure Certification Authority
  - Managing NVRAM Memory Usage
  - Configuring the Device Host Name and IP Domain Name
- Generating an RSA Key Pair
- Declaring a Certification Authority
- Configuring a Root CA (Trusted Root)
- Authenticating the CA
- Requesting Signed Certificates
- Monitoring and Maintaining Certification Authority
  - Requesting a Certificate Revocation List
  - Querying a Certification Revocation List
  - Deleting RSA Keys from a Device
  - Deleting Public Keys for a Peer
  - Deleting Certificates from the Configuration
- Viewing Keys and Certificates

### CHAPTER 41

**Access Control List Overview**

- Finding Feature Information
- Information About Access Control Lists
CHAPTER 42

Configuring IPv4 Access Control Lists  735
Finding Feature Information  735
Restrictions for Configuring IPv4 Access Control Lists  735
Information About Configuring IPv4 Access Control Lists  736
    ACL Overview  736
    Standard and Extended IPv4 ACLs  737
        IPv4 ACL Switch Unsupported Features  737
        Access List Numbers  737
    Numbered Standard IPv4 ACLs  738
    Numbered Extended IPv4 ACLs  739
    Named IPv4 ACLs  739
    Benefits of IP Access List Entry Sequence Numbering  740
        Sequence Numbering Behavior  740
Including comments in ACLs  741
Hardware and Software Treatment of IP ACLs  741
Time Ranges for ACLs  742
ACL Overview  772
IPv6 ACLs Overview  773
Interactions with Other Features and Switches  773
Default Configuration for IPv6 ACLs  773
Supported ACL Features  773
IPv6 Port-Based Access Control List Support  774
ACLs and Traffic Forwarding  774
How to Configure IPv6 ACLs  774
Configuring IPv6 ACLs  774
Attaching an IPv6 ACL to an Interface  778
Monitoring IPv6 ACLs  779
Configuring PACL Mode and Applying IPv6 PACL on an Interface  780
Configuring IPv6 ACL Extensions for Hop by Hop Filtering  781
Configuration Examples for IPv6 ACLs  782
Example: Configuring IPv6 ACLs  782
Example: Configuring PACL Mode and Applying IPv6 PACL on an Interface  782
Example: IPv6 ACL Extensions for Hop by Hop Filtering  782
Additional References  783
Feature Information for IPv6 Access Control Lists  784

CHAPTER 44  Configuring DHCP  787
Finding Feature Information  787
Information About DHCP  787
DHCP Server  787
DHCP Relay Agent  787
DHCP Snooping  788
Option-82 Data Insertion  789
Cisco IOS DHCP Server Database  792
DHCP Snooping Binding Database  792
How to Configure DHCP Features  794
Default DHCP Snooping Configuration  794
DHCP Snooping Configuration Guidelines  795
Configuring the DHCP Server  795
Configuring the DHCP Relay Agent  795
### Specifying the Packet Forwarding Address
- 796

### Prerequisites for Configuring DHCP Snooping and Option 82
- 798

### Enabling DHCP Snooping and Option 82
- 799

### Enabling the Cisco IOS DHCP Server Database
- 802

### Monitoring DHCP Snooping Information
- 803

### Configuring DHCP Server Port-Based Address Allocation
- 803

#### DHCP Server Port-Based Address Allocation
- 803

#### Default Port-Based Address Allocation Configuration
- 804

#### Port-Based Address Allocation Configuration Guidelines
- 804

#### Enabling the DHCP Snooping Binding Database Agent
- 804

#### Enabling DHCP Server Port-Based Address Allocation
- 806

#### Monitoring DHCP Server Port-Based Address Allocation
- 807

### Additional References
- 808

### Feature Information for DHCP Snooping and Option 82
- 808

---

**Chapter 45**

**Configuring IP Source Guard**

- 811

- Finding Feature Information
- 811

- Information About IP Source Guard
- 811

- IP Source Guard
- 811

- IP Source Guard for Static Hosts
- 812

- IP Source Guard Configuration Guidelines
- 812

- How to Configure IP Source Guard
- 813

- Enabling IP Source Guard
- 813

- Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port
- 814

- Monitoring IP Source Guard
- 816

- Additional References
- 817

---

**Chapter 46**

**Configuring IEEE 802.1x Port-Based Authentication**

- 819

- Finding Feature Information
- 819

- Information About 802.1x Port-Based Authentication
- 819

- Port-Based Authentication Process
- 820

- Port-Based Authentication Initiation and Message Exchange
- 822

- Authentication Manager for Port-Based Authentication
- 823

- Port-Based Authentication Methods
- 823
Per-User ACLs and Filter-Ids 824
Port-Based Authentication Manager CLI Commands 825
Ports in Authorized and Unauthorized States 826
802.1x Host Mode 827
802.1x Multiple Authentication Mode 828
MAC Move 828
MAC Replace 829
802.1x Accounting 829
802.1x Accounting Attribute-Value Pairs 830
Switch-to-RADIUS-Server Communication 831
802.1x Authentication with VLAN Assignment 831
802.1x Authentication with Guest VLAN 833
802.1x Authentication with Restricted VLAN 834
802.1x Auth Fail VLAN 834
802.1x Authentication with Inaccessible Authentication Bypass 835
  Inaccessible Authentication Bypass Support on Multiple-Authentication Ports 835
  Inaccessible Authentication Bypass Authentication Results 836
  Inaccessible Authentication Bypass Feature Interactions 836
802.1x Critical Voice VLAN 837
802.1x User Distribution 837
  802.1x User Distribution Configuration Guidelines 838
IEEE 802.1x Authentication with Voice VLAN Ports 838
IEEE 802.1x Authentication with Port Security 839
IEEE 802.1x Authentication with MAC Authentication Bypass 839
Per-User ACLs Authentication through 802.1x/MAB/WebAuth Users 840
Flexible Authentication Ordering 840
Open1x Authentication 841
Multidomain Authentication 841
Limiting Login for Users 843
Voice Aware 802.1x Security 843
How to Configure 802.1x Port-Based Authentication 843
  Default 802.1x Authentication Configuration 843
  802.1x Authentication Configuration Guidelines 845
  802.1x Authentication 845
VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass

MAC Authentication Bypass 846
Maximum Number of Allowed Devices Per Port 846
Configuring Voice Aware 802.1x Security 847
Configuring 802.1x Violation Modes 848
Configuring 802.1x Authentication 850
Configuring 802.1x Port-Based Authentication 851
Configuring the Switch-to-RADIUS-Server Communication 853
Configuring the Host Mode 854
Configuring Periodic Re-Authentication 856
Changing the Quiet Period 857
Changing the Switch-to-Client Retransmission Time 858
Setting the Switch-to-Client Frame-Retransmission Number 860
Setting the Re-Authentication Number 861
Enabling MAC Move 862
Enabling MAC Replace 863
Configuring 802.1x Accounting 864
Configuring a Guest VLAN 866
Configuring a Restricted VLAN 867
Configuring Number of Authentication Attempts on a Restricted VLAN 868
Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN 869
Example of Configuring Inaccessible Authentication Bypass 872
Configuring MAC Authentication Bypass 873
Formatting a MAC Authentication Bypass Username and Password 874
Configuring Per-User ACLs Authentication through 802.1x/MAB/WebAuth Users 875
Example: Per-User ACLs Authentication through 802.1x/MAB/WebAuth Users 877
Configuring Limiting Login for Users 877
Configuring 802.1x Auth Fail VLAN 878
Configuring the Number of Authentication Retries 880
Configuring Flexible Authentication Ordering 881
Configuring Open1x 882
Disabling 802.1x Authentication on the Port 884
Resetting the 802.1x Authentication Configuration to the Default Values 885
Monitoring 802.1x Statistics and Status 886
Additional References for IEEE 802.1x Port-Based Authentication 887
Feature Information for 802.1x Port-Based Authentication 888

CHAPTER 47

Configuring IPv6 First Hop Security 889
Finding Feature Information 889
Prerequisites for First Hop Security in IPv6 889
Restrictions for First Hop Security in IPv6 890
Information about First Hop Security in IPv6 890
How to Configure an IPv6 Snooping Policy 891
  How to Attach an IPv6 Snooping Policy to an Interface 893
  How to Attach an IPv6 Snooping Policy to a Layer 2 EtherChannel Interface 894
How to Configure the IPv6 Binding Table Content 895
How to Configure an IPv6 Neighbor Discovery Inspection Policy 897
  How to Attach an IPv6 Neighbor Discovery Inspection Policy to an Interface 898
  How to Attach an IPv6 Neighbor Discovery Inspection Policy to a Layer 2 EtherChannel Interface 899
How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on a Device 901
  How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on an Interface 901
  How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy to a Layer 2 EtherChannel Interface 902
How to Configure an IPv6 Router Advertisement Guard Policy 903
  How to Attach an IPv6 Router Advertisement Guard Policy to an Interface 906
  How to Attach an IPv6 Router Advertisement Guard Policy to a Layer 2 EtherChannel Interface 907
How to Configure an IPv6 DHCP Guard Policy 908
  How to Attach an IPv6 DHCP Guard Policy to an Interface or a VLAN on an Interface 910
  How to Attach an IPv6 DHCP Guard Policy to a Layer 2 EtherChannel Interface 911
How to Configure IPv6 Source Guard 912
  How to Attach an IPv6 Source Guard Policy to an Interface 914
  How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface 914
How to Configure IPv6 Prefix Guard 915
  How to Attach an IPv6 Prefix Guard Policy to an Interface 916
  How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface 917
Configuration Examples for IPv6 First Hop Security  918
  Examples: How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface  918
  Examples: How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface  918
Additional References  919

**CHAPTER 48**

Per-User ACL Support for 802.1X/MAB/Webauth Users  921
  Finding Feature Information  921
  Prerequisites for Per-User ACL Support for 802.1X/MAB/Webauth Users  921
  Restrictions for Per-User ACL Support for 802.1X/MAB/Webauth Users  922
  Information About Per-User ACL Support for 802.1X/MAB/Webauth Users  922
    802.1X Authentication with Per-User ACLs  922
  How to Configure Per-User ACL Support for 802.1X/MAB/Webauth Users  923
    Configuring Downloadable ACLs  923
  Configuration Examples for Per-User ACL Support for 802.1X/MAB/Webauth Users  924
    Example: Configuring a Switch for a Downloadable Policy  924
Additional References  925
  Feature Information for Per-User ACL Support for 802.1X/MAB/Webauth Users  926

**CHAPTER 49**

Web Authentication Redirection to Original URL  927
  Web Authentication Redirection to Original URL Overview  927
  Additional References for Web Authentication Redirection to Original URL  929
  Feature Information for Web Authentication Redirection to Original URL  929

**CHAPTER 50**

Configuring Web-Based Authentication  931
  Finding Feature Information  931
  Restrictions for Web-Based Authentication  931
  Information About Web-Based Authentication  931
    Web-Based Authentication Overview  931
  Device Roles  933
    Host Detection  933
    Session Creation  933
    Authentication Process  934
  Using Authentication Proxy  934
  When to Use the Authentication Proxy  935
How to Configure Port Security 978
  Enabling and Configuring Port Security 978
  Enabling and Configuring Port Security Aging 984
Configuration Examples for Port Security 985
Additional References 986
Finding Feature Information 987
Information About Protocol Storm Protection 987
  Protocol Storm Protection 987
  Default Protocol Storm Protection Configuration 988
How to Configure Protocol Storm Protection 988
  Enabling Protocol Storm Protection 988
  Monitoring Protocol Storm Protection 989
Additional References 989

PART IX

System Management 991

CHAPTER 52

Administering the System 993
  Information About Administering the Switch 993
    System Time and Date Management 993
    System Clock 993
    Real Time Clock 994
    Network Time Protocol 994
      NTP Stratum 995
      NTP Associations 996
      NTP Security 996
      NTP Implementation 996
      NTP Version 4 997
    System Name and Prompt 997
      Default System Name and Prompt Configuration 997
    DNS 997
      Default DNS Settings 998
    Login Banners 998
      Default Banner Configuration 998
    MAC Address Table 998

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
Boot Process  1025
Switches Information Assignment  1026
Default Switch Information  1026
DHCP-Based Autoconfiguration Overview  1027
  DHCP Client Request Process  1027
DHCP-based Autoconfiguration and Image Update  1028
  Restrictions for DHCP-based Autoconfiguration  1028
  DHCP Autoconfiguration  1029
  DHCP Auto-Image Update  1029
DHCP Server Configuration Guidelines  1029
  Purpose of the TFTP Server  1030
  Purpose of the DNS Server  1030
How to Obtain Configuration Files  1031
How to Control Environment Variables  1032
  Common Environment Variables  1033
Scheduled Reload of the Software Image  1034
How to Perform Switch Setup Configuration  1035
  Configuring DHCP Autoconfiguration (Only Configuration File)  1035
  Configuring DHCP Auto-Image Update (Configuration File and Image)  1037
  Configuring the Client to Download Files from DHCP Server  1040
Routing Assistance When IP Routing is Disabled  1041
  Default Gateway  1041
Manually Assigning IP Information to Multiple SVIs  1042
Configuring the NVRAM Buffer Size  1044
Modifying the Switch Startup Configuration  1045
  Specifying the Filename to Read and Write the System Configuration  1045
  Manually Booting the Switch  1046
  Configuring a Scheduled Software Image Reload  1047
Configuration Examples for Performing Switch Setup  1048
  Example: Configuring a Switch as a DHCP Server  1048
  Example: Configuring DHCP Auto-Image Update  1049
  Example: Configuring a Switch to Download Configurations from a DHCP Server  1049
  Example: Configuring NVRAM Buffer Size  1049
## CHAPTER 54  Configuring System Message Logs  1051

- Restrictions for Configuring System Message Logs  1051
- Information About Configuring System Message Logs  1051
  - System Message Logging  1051
  - System Log Message Format  1052
  - Default System Message Logging Settings  1053
  - Enabling Syslog Trap Messages  1053

### How to Configure System Message Logs  1054

- Setting the Message Display Destination Device  1054
- Synchronizing Log Messages  1055
- Disabling Message Logging  1057
- Enabling and Disabling Time Stamps on Log Messages  1058
- Enabling and Disabling Sequence Numbers in Log Messages  1058
- Defining the Message Severity Level  1059
- Limiting Syslog Messages Sent to the History Table and to SNMP  1060
- Logging Messages to a UNIX Syslog Daemon  1061

### Monitoring and Maintaining System Message Logs  1062

- Monitoring Configuration Archive Logs  1062
- Configuration Examples for System Message Logs  1062
  - Example: Switch System Message  1062
  - Examples: Displaying Service Timestamps Log  1063
- Additional References for System Message Logs  1063
- Feature History and Information For System Message Logs  1064

## CHAPTER 55  Configuring Online Diagnostics  1065

- Information About Configuring Online Diagnostics  1065
  - Online Diagnostics  1065

### How to Configure Online Diagnostics  1066

- Starting Online Diagnostic Tests  1066
- Configuring Online Diagnostics  1066
- Scheduling Online Diagnostics  1066
- Configuring Health-Monitoring Diagnostics  1067

### Monitoring and Maintaining Online Diagnostics  1070
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying Online Diagnostic Tests and Test Results</td>
<td>1070</td>
</tr>
<tr>
<td>Configuration Examples for Online Diagnostic Tests</td>
<td>1070</td>
</tr>
<tr>
<td>Starting Online Diagnostic Tests</td>
<td>1070</td>
</tr>
<tr>
<td>Example: Configure a Health Monitoring Test</td>
<td>1071</td>
</tr>
<tr>
<td>Examples: Schedule Diagnostic Test</td>
<td>1071</td>
</tr>
<tr>
<td>Displaying Online Diagnostics: Examples</td>
<td>1072</td>
</tr>
<tr>
<td>Troubleshooting the Software Configuration</td>
<td>1075</td>
</tr>
<tr>
<td>Information About Troubleshooting the Software Configuration</td>
<td>1075</td>
</tr>
<tr>
<td>Software Failure on a Switch</td>
<td>1075</td>
</tr>
<tr>
<td>Lost or Forgotten Password on a Switch</td>
<td>1075</td>
</tr>
<tr>
<td>Power over Ethernet Ports</td>
<td>1076</td>
</tr>
<tr>
<td>Disabled Port Caused by Power Loss</td>
<td>1076</td>
</tr>
<tr>
<td>Disabled Port Caused by False Link-Up</td>
<td>1077</td>
</tr>
<tr>
<td>Ping</td>
<td>1077</td>
</tr>
<tr>
<td>Layer 2 Traceroute</td>
<td>1077</td>
</tr>
<tr>
<td>Layer 2 Traceroute Guidelines</td>
<td>1077</td>
</tr>
<tr>
<td>IP Traceroute</td>
<td>1078</td>
</tr>
<tr>
<td>Time Domain Reflector Guidelines</td>
<td>1079</td>
</tr>
<tr>
<td>Debug Commands</td>
<td>1080</td>
</tr>
<tr>
<td>Onboard Failure Logging on the Switch</td>
<td>1080</td>
</tr>
<tr>
<td>Possible Symptoms of High CPU Utilization</td>
<td>1081</td>
</tr>
<tr>
<td>How to Troubleshoot the Software Configuration</td>
<td>1081</td>
</tr>
<tr>
<td>Recovering from a Software Failure</td>
<td>1081</td>
</tr>
<tr>
<td>Recovering from a Lost or Forgotten Password</td>
<td>1083</td>
</tr>
<tr>
<td>Procedure with Password Recovery Enabled</td>
<td>1084</td>
</tr>
<tr>
<td>Procedure with Password Recovery Disabled</td>
<td>1086</td>
</tr>
<tr>
<td>Recovering from a Command Switch Failure</td>
<td>1088</td>
</tr>
<tr>
<td>Replacing a Failed Command Switch with a Cluster Member</td>
<td>1088</td>
</tr>
<tr>
<td>Replacing a Failed Command Switch with Another Switch</td>
<td>1090</td>
</tr>
<tr>
<td>Preventing Autonegotiation Mismatches</td>
<td>1091</td>
</tr>
<tr>
<td>Troubleshooting SFP Module Security and Identification</td>
<td>1091</td>
</tr>
<tr>
<td>Monitoring SFP Module Status</td>
<td>1092</td>
</tr>
<tr>
<td>Executing Ping</td>
<td>1092</td>
</tr>
</tbody>
</table>
Monitoring Temperature 1092
Monitoring the Physical Path 1093
Executing IP Traceroute 1093
Running TDR and Displaying the Results 1093
Redirecting Debug and Error Message Output 1093
Using the show platform forward Command 1094
Configuring OBFL 1094
Verifying Troubleshooting of the Software Configuration 1095
Displaying OBFL Information 1095
Example: Verifying the Problem and Cause for High CPU Utilization 1096
Scenarios for Troubleshooting the Software Configuration 1098
Scenarios to Troubleshoot Power over Ethernet (PoE) 1098
Configuration Examples for Troubleshooting Software 1100
Example: Pinging an IP Host 1100
Example: Performing a Traceroute to an IP Host 1101
Example: Enabling All System Diagnostics 1102
Additional References for Troubleshooting Software Configuration 1102
Feature History and Information for Troubleshooting Software Configuration 1103

PART X

Working with the Cisco IOS File System, Configuration Files, and Software Images 1105

CHAPTER 57

Working with the Cisco IOS File System, Configuration Files, and Software Images 1107
Working with the Flash File System 1107
Information About the Flash File System 1107
Displaying Available File Systems 1107
Setting the Default File System 1109
Displaying Information About Files on a File System 1109
Changing Directories and Displaying the Working Directory 1110
Creating Directories 1111
Removing Directories 1111
Copying Files 1112
Deleting Files 1112
Creating, Displaying and Extracting Files 1113
Working with Configuration Files 1114
Preface

This book describes configuration information and examples for on the switch.

- Document Conventions, on page lv
- Obtaining Documentation and Submitting a Service Request, on page lvii

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 <strong>bold</strong> 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 <em>italic</em> font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> 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>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
</tbody>
</table>
### Convention | Description
--- | ---
[x {y | z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<> | Nonprinting characters such as passwords are in angle brackets.
[ ] | Default responses to system prompts are in square brackets.
!, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

---

**Reader Alert Conventions**

This document may use the following conventions for reader alerts:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td><em>Means reader take note.</em> Notes contain helpful suggestions or references to material not covered in the manual.</td>
</tr>
<tr>
<td>Tip</td>
<td><em>Means the following information will help you solve a problem.</em></td>
</tr>
<tr>
<td>Caution</td>
<td><em>Means reader be careful.</em> In this situation, you might do something that could result in equipment damage or loss of data.</td>
</tr>
<tr>
<td>Timesaver</td>
<td><em>Means the described action saves time.</em> You can save time by performing the action described in the paragraph.</td>
</tr>
</tbody>
</table>
| 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 |
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.
Using the Command-Line Interface

- Information About Using the Command-Line Interface, on page 1
- How to Use the CLI to Configure Features, on page 5

Information About Using the Command-Line Interface

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

Command Modes

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

You can start a CLI session through a console connection, through Telnet, an SSH, or by using the browser. When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as show commands, which show the current configuration status, and clear commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

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

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

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.
Table 1: Command Mode Summary

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
</table>
| User EXEC           | Begin a session using Telnet, SSH, or console.                                | Switch>               | Enter logout or quit | Use this mode to
• Change terminal settings.  
• Perform basic tests.  
• Display system information. |
| Privileged EXEC     | While in user EXEC mode, enter the enable command.                            | Switch#               | Enter disable to exit.| Use this mode to verify commands that you have entered. Use a password to protect access to this mode.                                               |
| Global configuration| While in privileged EXEC mode, enter the configure command.                   | Switch(config)#       | To exit to privileged EXEC mode, enter exit or end, or press Ctrl-Z. | Use this mode to configure parameters that apply to the entire switch.                                                                             |
| VLAN configuration  | While in global configuration mode, enter the **vlan vlan-id** command.       | Switch(config-vlan)#  | To exit to global configuration mode, enter the exit command.  
To return to privileged EXEC mode, press Ctrl-Z or enter end. | Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file. |
### Understanding Abbreviated Commands

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

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

```
Switch# show conf
```

### No and Default Forms of Commands

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

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

### CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.
Table 2: Common CLI Error Messages

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

Configuration Logging

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

Note

Only CLI or HTTP changes are logged.

Using the Help System

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

SUMMARY STEPS

1. help
2. abbreviated-command-entry ?
3. abbreviated-command-entry <Tab>
4. ?
5. command ?
6. command keyword ?
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>help</td>
<td>Obtains a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# help</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>abbreviated-command-entry ?</td>
<td>Obtains a list of commands that begin with a particular character string.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# di? dir disable disconnect</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>abbreviated-command-entry &lt;Tab&gt;</td>
<td>Completes a partial command name.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# sh conf&lt;tab&gt; Switch# show configuration</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>?</td>
<td>Lists all commands available for a particular command mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; ?</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>command ?</td>
<td>Lists the associated keywords for a command.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; show ?</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>command keyword ?</td>
<td>Lists the associated arguments for a keyword.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# cdp holdtime ? &lt;10-255&gt; Length of time (in sec) that receiver must keep this packet</td>
<td></td>
</tr>
</tbody>
</table>

How to Use the CLI to Configure Features

Configuring the Command History

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

Changing the Command History Buffer Size

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

1. **terminal history [size number-of-lines]**

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><strong>terminal history [size number-of-lines]</strong></td>
<td>Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# <strong>terminal history size 200</strong></td>
<td></td>
</tr>
</tbody>
</table>

Recalling Commands

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

**Note**

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

SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

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><strong>Ctrl-P</strong> or use the <strong>up arrow</strong> key</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>Ctrl-N</strong> or use the <strong>down arrow</strong> key</td>
<td>Returns to more recent commands in the history buffer after recalling commands with <strong>Ctrl-P</strong> or the up arrow key. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>show history</strong></td>
<td>Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the <strong>terminal history</strong> global configuration command and the <strong>history</strong> line configuration command.</td>
</tr>
</tbody>
</table>

Example:

Switch# **show history**

Disabling the Command History Feature

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

1. terminal no history

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 terminal no history</td>
<td>Disables the feature during the current terminal session in privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Example:

Switch# terminal no history

Enabling and Disabling Editing Features

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

SUMMARY STEPS

1. terminal editing
2. terminal no editing

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 terminal editing</td>
<td>Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Example:

Switch# terminal editing

Step 2 terminal no editing | Disables the enhanced editing mode for the current terminal session in privileged EXEC mode. |

Example:

Switch# terminal no editing

Editing Commands Through Keystrokes

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

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

<table>
<thead>
<tr>
<th>Editing Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-B or use the left arrow key</td>
<td>Moves the cursor back one character.</td>
</tr>
<tr>
<td>Ctrl-F or use the right arrow key</td>
<td>Moves the cursor forward one character.</td>
</tr>
<tr>
<td>Key Combination</td>
<td>Action</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
</tr>
<tr>
<td>Ctrl-A</td>
<td>Moves the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl-E</td>
<td>Moves the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Esc B</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc F</td>
<td>Moves the cursor forward one word.</td>
</tr>
<tr>
<td>Ctrl-T</td>
<td>Transposes the character to the left of the cursor with the character located at the cursor.</td>
</tr>
<tr>
<td>Delete or Backspace key</td>
<td>Erases the character to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl-D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Ctrl-K</td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl-U or Ctrl-X</td>
<td>Deletes all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl-W</td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Esc D</td>
<td>Deletes from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Esc C</td>
<td>Capitalizes at the cursor.</td>
</tr>
<tr>
<td>Esc L</td>
<td>Changes the word at the cursor to lowercase.</td>
</tr>
<tr>
<td>Esc U</td>
<td>Capitalizes letters from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Ctrl-V or Esc Q</td>
<td>Designates a particular keystroke as an executable command, perhaps as a shortcut.</td>
</tr>
<tr>
<td>Return key</td>
<td>Scrolls down a line or screen on displays that are longer than the terminal screen can display. <strong>Note</strong> The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including <code>show</code> command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.</td>
</tr>
<tr>
<td>Space bar</td>
<td>Scrolls down one screen.</td>
</tr>
<tr>
<td>Ctrl-L or Ctrl-R</td>
<td>Redisplays the current command line if the switch suddenly sends a message to your screen.</td>
</tr>
</tbody>
</table>

### Editing Command Lines That Wrap

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

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.
The arrow keys function only on ANSI-compatible terminals such as VT100s.

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

**SUMMARY STEPS**

1. access-list
2. Ctrl-A
3. Return key

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** access-list  
Example:  
Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35  
Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35  
Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq  
Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45  
| Displays the global configuration command entry that extends beyond one line.  
When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left. |
| **Step 2** Ctrl-A  
Example:  
Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$  
| Checks the complete syntax.  
The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right. |
| **Step 3** Return key  
| Execute the commands.  
The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the **terminal width** privileged EXEC command to set the width of your terminal.  
Use line wrapping with the command history feature to recall and modify previous complex command entries. |

**Searching and Filtering Output of show and more Commands**

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

1. \{show \| more\} command \| \{begin \| include \| exclude\} regular-expression

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> {show | more} command | {begin | include | exclude} regular-expression</td>
<td>Searches and filters the output. Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output are not displayed, but the lines that contain output appear.</td>
</tr>
</tbody>
</table>
| Example: Switch\# show interfaces \| include protocol  
Vlan1 is up, line protocol is up  
Vlan10 is up, line protocol is down  
GigabitEthernet0/1 is up, line protocol is down  
GigabitEthernet0/2 is up, line protocol is up | |

Accessing the CLI Through a Console Connection or Through Telnet

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

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

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

**Procedure**

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

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

Accessing the CLI through Bluetooth

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

**Note**  
This feature is available on Cisco IOS Release 15.2(5)E2 and higher.
1. Connect a Bluetooth dongle to the USB port on your switch and power on the switch.

2. Turn on Bluetooth on your computer and discover the switch.

3. Pair the computer to the switch.

4. Connect to the switch as an access point.
   - If you are connecting from a Windows computer: Go to Devices & Printers, select the switch, click on the Connect Using tab and select Access point.
   - If you are connecting from a Mac computer: On the menu bar, click the Bluetooth icon, hover over the switch name, and click Connect to Network.

Once a connection is established, you can open a management window and configure the switch.
Accessing the CLI through Bluetooth
PART

Interface and Hardware

• Configuring Interface Characteristics, on page 15
• Configuring Auto-MDIX, on page 39
• Configuring LLDP, LLDP-MED, and Wired Location Service, on page 43
• Configuring System MTU, on page 57
• Configuring PoE, on page 61
• Configuring EEE, on page 77
Configuring Interface Characteristics

- Finding Feature Information, on page 15
- Information About Configuring Interface Characteristics, on page 15
- How to Configure Interface Characteristics, on page 23
- Monitoring Interface Characteristics, on page 34
- Configuration Examples for Interface Characteristics, on page 35
- Additional References for the Interface Characteristics Feature, on page 37
- Feature History and Information for Configuring Interface Characteristics, on page 38

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.

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.

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.

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.

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.

**Routed Ports**

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as DTP and STP.

Configure routed ports by putting the interface into Layer 3 mode with the `no switchport` interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the `ip routing` and `router protocol` global configuration commands.

Note

Entering a `no switchport` interface configuration command shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost.

The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations.

**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.

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 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.

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]

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).
- **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.

### Default Ethernet Interface Configuration

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

**Table 4: Default Layer 2 Ethernet Interface Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating mode</td>
<td>Layer 2 or switching mode (<a href="#"><code>switchport</code> command</a>).</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>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>
</tbody>
</table>
### Feature | Default Setting
--- | ---
Port blocking (unknown multicast and unknown unicast traffic) | Disabled (not blocked).
Broadcast, multicast, and unicast storm control | Disabled.
Protected port | Disabled.
Port security | Disabled.
Port Fast | Disabled.
Auto-MDIX | Enabled. **Note** The 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.
Power over Ethernet (PoE) | Enabled (auto).
Keepalive messages | Disabled on SFP module ports; enabled on all other ports.

### Interface Speed and Duplex Mode

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

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

### Speed and Duplex Configuration Guidelines

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

- Do not disable Auto-Negotiation on PoE switches.
- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.
- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
  - The 1000BASE-x (where -x is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the **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.
• Catalyst 2960-L Switches do not support GLC-T and GLC-TE at speed 10/100 Mb/s.

Note

• 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.

Note

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.

**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><strong>Example:</strong></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><strong>Example:</strong></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 and the number of the connector.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>• 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 <code>gigabitethernet 0/1</code>, <code>gigabitethernet0/1</code>, <code>gi 0/1</code>, or <code>gi0/1</code>.</td>
</tr>
<tr>
<td></td>
<td>Switch{config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch{config-if)#</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Follow each interface command with the interface configuration commands that the interface requires.</td>
<td>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 <strong>end</strong> to return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>interface range</strong> or <strong>interface range macro</strong></td>
<td>(Optional) Configures a range of interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
<td>Interfaces configured in a range must be the same type and must be configured with the same feature options.</td>
</tr>
<tr>
<td></td>
<td>Display 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.</td>
<td></td>
</tr>
</tbody>
</table>
# 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> 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 interface for which you are adding a description, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> description string</td>
<td>Adds a description (up to 240 characters) for an interface.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# description Connects to Marketing</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-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show interfaces interface-id description</td>
<td>Verifies your entry.</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><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>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 range {port-range</td>
<td>macro macro_name}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• You can use the <code>interface range</code> command to configure up to five port ranges or a previously defined macro.</td>
</tr>
<tr>
<td>Switch(config)# interface range macro</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The <code>macro</code> variable is explained in the section on Configuring and Using Interface Range Macros.</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

<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>Example: 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: 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: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
### 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:*  
  `Switch> enable` |
| 2    | configure terminal | Enters global configuration mode.  
  *Example:*  
  `Switch# configure terminal` |
| 3    | define interface-range `macro_name` interface-range | Defines the interface-range macro, and save it in NVRAM.  
  *Example:*  
  `Switch(config)# define interface-range enet_list gigabitethernet 0/1 - 2`  
  *Note:* Before you can use the `macro` keyword in the `interface range macro` global configuration command string, you must use the `define interface-range` global configuration command to define the macro. |
| 4    | interface range macro `macro_name`  
  *Example:*  
  `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.  
  *Note:*  
  - The `macro_name` is a 32-character maximum character string.  
  - A macro can contain up to five comma-separated interface ranges.  
  - Each `interface-range` must consist of the same port type. |
| 5    | end               | Returns to privileged EXEC mode.  
  *Example:*  
  `Switch(config)# end` |
| 6    | show running-config | include define  
  *Example:*  
  `Switch# show running-config | include define`  
  Shows the defined interface range macro configuration. |
### 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><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 interface-id</td>
<td>Specifies the physical interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> speed {10</td>
<td>100</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter 10, 100, 1000 to set a specific speed for the interface.</td>
</tr>
</tbody>
</table>
**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>Enters global configuration mode</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the physical interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the flow control mode for the port.</td>
</tr>
<tr>
<td>flowcontrol {receive} {on</td>
<td>off</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# flowcontrol receive on</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies the interface flow control settings.</td>
</tr>
<tr>
<td>show interfaces interface-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# show interfaces gigabitethernet 0/1</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></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

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
### Interface and Hardware

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> enable</td>
<td></td>
</tr>
</tbody>
</table>
| 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 {vlan vlan-id} | Selects the interface to be configured.  
| | {gigabitethernet interface-id}  
| | | {port-channel port-channel-number} |
| Example: Switch(config)# interface gigabitethernet 0/2 |
| **Step 4** shutdown  |
| Example: Switch(config-if)# shutdown | Shuts down an interface. |
| **Step 5** no shutdown  |
| Example: Switch(config-if)# no shutdown | Restarts an interface. |
| **Step 6** end  |
| Example: Switch(config-if)# end | Returns to privileged EXEC mode. |
| **Step 7** show running-config  |
| Example: | Verifies your entries. |
Configuring the Console Media Type

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

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>&lt;br&gt;enable&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch&gt; enable</td>
<td>Enables privileged EXEC mode. <em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;configure terminal&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;line console 0&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config)# line console 0</td>
<td>Configures the console and enters line configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;media-type rj45&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config-line)# media-type rj45</td>
<td>Configures the console media type to be only RJ-45 port. If you do not enter this command and both RJ-45 port and both types are connected, the USB port is used by default.</td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;end&lt;br&gt;<strong>Example:</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# end</td>
<td></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.

### 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.

**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><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>
</tbody>
</table>

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

| Step 3 line console 0     | Configures the console and enters line configuration mode.              |
| Example:                  |                                                                         |
| Switch(config)# line console 0 |                                                                       |
Step 4  usb-inactivity-timeout timeout-minutes
Example: Switch(config-line)# usb-inactivity-timeout 30

Step 5  copy running-config startup-config
Example: Switch# copy running-config startup-config

Monitoring Interface Characteristics

Monitoring Interface Status

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

Table 5: Show Commands for Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces interface-number downshift module module-number</td>
<td>Displays the downshift status details of the specified interfaces and modules.</td>
</tr>
<tr>
<td>show interfaces interface-id status [err-disabled]</td>
<td>Displays interface status or a list of interfaces in the error-disabled state.</td>
</tr>
<tr>
<td>show interfaces [interface-id] switchport</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>show interfaces [interface-id] description</td>
<td>Displays the description configured on an interface or all interfaces and the interface status.</td>
</tr>
<tr>
<td>show ip interface [interface-id]</td>
<td>Displays the usability status of all interfaces configured for IP routing or the specified interface.</td>
</tr>
<tr>
<td>show interface [interface-id] stats</td>
<td>Displays the input and output packets by the switching path for the interface.</td>
</tr>
<tr>
<td>show interfaces interface-id</td>
<td>(Optional) Displays speed and duplex on the interface.</td>
</tr>
<tr>
<td>show interfaces transceiver dom-supported-list</td>
<td>(Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules.</td>
</tr>
</tbody>
</table>
### Clearing and Resetting Interfaces and Counters

**Table 6: Clear Commands for Interfaces**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters [interface-id]</td>
<td>Clears interface counters.</td>
</tr>
<tr>
<td>clear interface interface-id</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
```

### 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 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

#### 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 the 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 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 3

Configuring Auto-MDIX

- Prerequisites for Auto-MDIX, on page 39
- Restrictions for Auto-MDIX, on page 39
- Information About Configuring Auto-MDIX, on page 39
- How to Configure Auto-MDIX, on page 40
- Example for Configuring Auto-MDIX, on page 41
- Additional References, on page 42
- Feature History and Information for Auto-MDIX, on page 42

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 7: 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: <code>enable</code></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: <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies the physical interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: <code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<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>Configures the interface to autonegotiate speed with the connected device.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# speed auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> duplex auto</td>
<td>Configures 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

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the 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 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring LLDP, LLDP-MED, and Wired Location Service

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 LLDP, LLDP-MED, and Wired Location Service

LLDP

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

To support non-Cisco devices and to allow for interoperability between other devices, the 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.

**LLDP-MED**

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

**LLDP-MED Supported TLVs**

LLDP-MED supports these TLVs:

- LLDP-MED capabilities TLV
  Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.
- Network policy TLV
  Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. For example, the switch can notify a phone of the VLAN number that it should use. The phone can connect to any 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 about the manufacturer, model, 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 8: 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>
</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` command on the interface. If the `switchport voice vlan vlan-id` is already configured on an interface, you can apply a network-policy profile on the interface. This way the interface has the voice or voice-signaling VLAN network-policy profile applied on the interface.

- You cannot configure static secure MAC addresses on an interface that has a network-policy profile.

- When Cisco Discovery Protocol and LLDP are both in use within the same switch, it is necessary to disable LLDP on interfaces where Cisco Discovery Protocol is in use for power negotiation. LLDP can be disabled at interface level with the commands `no lldp tlv-select power-management` or `no lldp transmit / no lldp receive`.

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

### Enabling LLDP

**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><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>
</tbody>
</table>

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

| **Step 3** lldp run | Enables LLDP globally on the switch. |
| **Example:** Switch (config)# lldp run | |

| **Step 4** interface interface-id | Specifies the interface on which you are enabling LLDP, and enter interface configuration mode. |
| **Example:** Switch (config)# interface gigabitethernet 0/1 | |

| **Step 5** lldp transmit | Enables the interface to send LLDP packets. |
| **Example:** Switch(config-if)# lldp transmit | |

| **Step 6** lldp receive | Enables the interface to receive LLDP packets. |
| **Example:** Switch(config-if)# lldp receive | |

| **Step 7** end | Returns to privileged EXEC mode. |
| **Example:** Switch(config-if)# end | |

| **Step 8** show lldp | Verifies the configuration. |
| **Example:** Switch# show lldp | |
### 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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
</tbody>
</table>

- Enter your password if prompted.

<p>| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | Switch# <code>configure terminal</code> | |</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 9: LLDP-MED TLVs

<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>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>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------</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>Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies the TLV to enable.</td>
</tr>
<tr>
<td><code>lldp med-tlv-select</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# lldp med-tlv-select inventory management</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</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>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></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>

### 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`
## 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><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

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

| **Step 3** network-policy profile profile number | Specifies the network-policy profile number, and enter network-policy configuration mode. The range is 1 to 4294967295. |
| **Example:** Switch(config)# network-policy profile 1 |

<p>| <strong>Step 4</strong> {voice | voice-signaling} vlan [vlan-id {cos cvalue | dscp dvalue}] | Configures the policy attributes: |
| <strong>Example:</strong> Switch(config-network-policy)# voice vlan 100 cos 4 | • voice—Specifies the voice application type. |
| | • voice-signaling—Specifies the voice-signaling application type. |
| | • vlan—Specifies the native VLAN for voice traffic. |
| | • vlan-id—(Optional) Specifies the VLAN for voice traffic. The range is 1 to 4094. |
| | • cos cvalue—(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5. |
| | • dscp dvalue—(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46. |
| | • dot1p—(Optional) Configures the telephone to use IEEE 802.1p priority tagging and use VLAN 0 (the native VLAN). |
| | • none—(Optional) Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad. |
| | • untagged—(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>untagged</strong></td>
<td><em>(Optional)</em> Configures the telephone to send untagged voice traffic. This is the default for the telephone.</td>
</tr>
</tbody>
</table>

**Step 5**

**exit**

Example:

```
Switch(config)# exit
```

Returns to global configuration mode.

**Step 6**

**interface interface-id**

Example:

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

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

**Step 7**

**network-policy profile number**

Example:

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

Specifies the network-policy profile number.

**Step 8**

**lldp med-tlv-select network-policy**

Example:

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

Specifies the network-policy TLV.

**Step 9**

**end**

Example:

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

Returns to privileged EXEC mode.

**Step 10**

**show network-policy profile**

Example:

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

Verifies the configuration.

**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>
</tbody>
</table>
### Command and Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `show lldp interface [interface-id]` | Displays information about interfaces with LLDP enabled.  
You can limit the display to a specific interface. |
| `show lldp neighbors [interface-id] [detail]` | Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID.  
You can limit the display to neighbors of a specific interface or expand the display for more detailed information. |
| `show lldp traffic`          | Displays LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs. |
| `show location admin-tag string` | Displays the location information for the specified administrative tag or site. |
| `show location civic-location identifier id` | Displays the location information for a specific global civic location. |
| `show location elin-location identifier id` | Displays the location information for an emergency location |
| `show network-policy profile` | Displays the configured network-policy profiles. |
| `show nmsp`                  | Displays the NMSP information |

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

#### MIBs

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

<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 LLDP, LLDP-MED, and Wired Location Service

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring System MTU

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. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the `system mtu jumbo` global configuration command.

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>
<tbody>
<tr>
<td><strong>Step 1</strong> <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> <code>system mtu bytes</code></td>
<td>Enter 1500, 2026 or jumbo to specify the MTU size. The MTU value of jumbo is 10218.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# system mtu 1500</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>system mtu jumbo</code></td>
<td>Enter 1500, 2026 or jumbo to specify the MTU size. The MTU value of jumbo is 10218.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# system mtu jumbo</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <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 5</strong> <code>copy running-config startup-config</code></td>
<td>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><strong>Step 6</strong> <code>do show system mtu</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# do show system mtu</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples for System MTU

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

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

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

```
Switch# show system mtu
```
System MTU size is 1500 bytes.
Configuration Examples for System MTU
Configuring PoE

- Finding Feature Information, on page 61
- Information About PoE, on page 61
- How to Configure PoE, on page 66
- Monitoring Power Status, on page 75
- Configuration Examples for Configuring PoE, on page 75

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 PoE

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.

Supported Protocols and Standards

The switch uses these protocols and standards to support PoE:
• CDP with power consumption—The powered device notifies the switch of the amount of power it is consuming. The switch does not reply to the power-consumption messages. The switch can only supply power to or remove power from the PoE port.

• Cisco intelligent power management—The powered device and the switch negotiate through power-negotiation CDP messages for an agreed-upon power-consumption level. The negotiation allows a high-power Cisco powered device, which consumes more than 7 W, to operate at its highest power mode. The powered device first boots up in low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in high-power mode. The device changes to high-power mode only when it receives confirmation from the switch.

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

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

• IEEE 802.3af—The major features of this standard are powered-device discovery, power administration, disconnect detection, and optional powered-device power classification. For more information, see the standard.

Powered-Device Detection and Initial Power Allocation

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

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

• The initial power allocation is the maximum amount of power that a powered device requires. The switch initially allocates this amount of power when it detects and powers the powered device. As the switch receives CDP messages from the powered device and as the powered device negotiates power levels with the switch through CDP power-negotiation messages, the initial power allocation might be adjusted.

• The switch classifies the detected IEEE device within a power consumption class. Based on the available power in the power budget, the switch determines if a port can be powered. Table 10: IEEE Power Classifications, on page 62 lists these levels.

<table>
<thead>
<tr>
<th>Class</th>
<th>Maximum Power Level Required from the Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (class status unknown)</td>
<td>15.4 W</td>
</tr>
<tr>
<td>1</td>
<td>4 W</td>
</tr>
<tr>
<td>2</td>
<td>7 W</td>
</tr>
<tr>
<td>3</td>
<td>15.4 W</td>
</tr>
<tr>
<td>4</td>
<td>30 W (For IEEE 802.3at Type 2 powered devices)</td>
</tr>
</tbody>
</table>
The switch monitors and tracks requests for power and grants power only when it is available. The switch tracks its power budget (the amount of power available on the switch for PoE). The switch performs power-accounting calculations when a port is granted or denied power to keep the power budget up to date.

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

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

---

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

---

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

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

### Power Management Modes

The switch supports these PoE modes:

- **auto**—The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch has enough power, it grants power, updates the power budget, turns on power to the port on a first-come, first-served basis, and updates the LEDs. For LED information, see the hardware installation guide.

  If the switch has enough power for all the powered devices, they all come up. If enough power is available for all powered devices connected to the switch, power is turned on to all devices. If there is not enough available PoE, or if a device is disconnected and reconnected while other devices are waiting for power, it cannot be determined which devices are granted or are denied power.

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

  If a device being powered by the switch is then connected to wall power, the switch might continue to power the device. The switch might continue to report that it is still powering the device whether the device is being powered by the switch or receiving power from an AC power source.
If a powered device is removed, the switch automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

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

- **static**—The switch pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. The switch allocates the port configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come, first-served model.

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

---

**Note**

In interface mode, the power consumption of a device cannot exceed the power supplied to the static port.

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

- **never**—The switch disables powered-device detection and never powers the PoE port even if an unpowered device is connected. Use this mode only when you want to make sure that power is never applied to a PoE-capable port, making the port a data-only port.

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

**Power Monitoring and Power Policing**

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

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

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

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

1. The switch monitors the real-time power consumption on individual ports.
2. The switch records the power consumption, including peak power usage. The switch reports the information through the CISCO-POWER-ETHERNET-EXT-MIB.
3. If power policing is enabled, the switch polices power usage by comparing the real-time power consumption to the maximum power allocated to the device. The maximum power consumption is also referred to as the cutoff power on a PoE port. If the device uses more than the maximum power allocation on the port, the switch can either turn off power to the port, or the switch can generate a syslog message and update the LEDs (the port LED is now blinking amber) while still providing power to the device based on the switch configuration. By default, power-usage policing is disabled on all PoE ports.

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

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

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

Maximum Power Allocation (Cutoff Power) on a PoE Port

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

1. Manually when you set the user-defined power level that limits the power allowed on the port by using the `power inline auto max max-wattage` or the `power inline static max max-wattage` interface configuration command

2. Automatically when the switch sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

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

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

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

Power Consumption Values

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

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

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

---

**Note**
In interface mode, the power consumption of a device cannot exceed the power supplied to the static port.

For example, if you configure power supply to the port at 6000 mW (`power inline static6000` interface configuration command), do not configure power consumption by a device at 8000 mW on the same port (`power inline consumption8000` interface configuration command).

---

**Persistent PoE**

Persistent PoE provides uninterrupted power to connected devices even when the switch is booting.

---

**Note**
Persistent PoE is supported on Catalyst 2960-L switches from Cisco IOS Release 15.2(5)E2 and higher.

---

**How to Configure PoE**

**Configuring a Power Management Mode on a PoE Port**

---

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

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `power inline [auto [max max-wattage] | never | static [max max-wattage]]`
5. `end`
6. `show power inline [interface-id | module switch-number]`
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 |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** interface interface-id | Specifies the physical port to be configured, and enters interface configuration mode.  
  Example:  
  Switch(config)# interface gigabitethernet 0/1 |
| **Step 4** power inline [auto [max max-wattage] | never | static [max max-wattage]] | Configures the PoE mode on the port. The keywords have these meanings:  
  • auto—Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. This is the default setting.  
  • max max-wattage—Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed.  
  • never —Disables device detection, and disable power to the port.  
  **Note** If a port has a Cisco powered device connected to it, do not use the **power inline never** command to configure the port. A false link-up can occur, placing the port into the error-disabled state.  
  • static—Enables powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers |
### Configuring Persistent PoE

**Persistent PoE** is supported in Catalyst 2960-L switches from Cisco IOS Release 15.2(5)E2 and higher.

To configure persistent 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`.

If you want to reload the switch, ensure that the persistent PoE configuration is first saved. This is necessary to preserve the configuration.

**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>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>Example: <code>Switch&gt; 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></td>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface interface-id</code></td>
<td>Specifies the physical port to be configured, 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>Step 4</td>
<td><code>power inline port poe-ha</code></td>
<td>Configures persistent PoE.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# power inline port poe-ha</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>Example: <code>Switch(config-if)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Budgeting Power for Devices Connected to a PoE Port**

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

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

⚠️

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

⚠️

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

⚠️

**Note**
In interface mode, the power consumption of a device cannot exceed the power supplied to the static port. For example, if you configure power supply to the port at 6000 mW (power inline static6000 interface configuration command), do not configure power consumption by a device at 8000 mW on the same port (power inline consumption8000 interface configuration command).

### Budgeting Power to All PoE ports

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cdp run**
4. **power inline consumption default** *wattage*
5. **end**
6. **show power inline consumption default**
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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Switch&gt; enable</strong></td>
<td></td>
</tr>
</tbody>
</table>

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

| **Step 3**        | (Optional) Disables CDP. |
| **no cdp run**    | |
| **Example:**      | |
### Command or Action

**Switch(config)# no cdp run**

**Purpose**

Enables privileged EXEC mode.

@Step 4

**power inline consumption default wattage**

**Example:**

Switch(config)# power inline consumption default 5000

Configures the power consumption of powered devices connected to each PoE port.

The range for each device is 4000 to 30000 mW (PoE+). The default is 30000 mW.

**Step 5**

**end**

**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

**Step 6**

**show power inline consumption default**

**Example:**

Switch# show power inline consumption default

Displays the power consumption status.

**Step 7**

**copy running-config startup-config**

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

### Budgeting Power to a Specific PoE Port

**SUMMARY STEPS**

1. enable
2. configure terminal
3. no cdp run
4. interface interface-id
5. power inline consumption wattage
6. end
7. show power inline consumption
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
| Example: Switch> enable |
| Enables privileged EXEC mode.
| • Enter your password if prompted. |
| **Step 2**
| configure terminal
<p>| Example: |
| Enters global configuration mode. |</p>
<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
- **no cdp run**
  - **Example:**
    ```
    Switch(config)# no cdp run
    ```
  - (Optional) Disables CDP.

Step 4
- **interface interface-id**
  - **Example:**
    ```
    Switch(config)# interface gigabitethernet 0/1
    ```
  - Specifies the physical port to be configured, and enter interface configuration mode.

Step 5
- **power inline consumption wattage**
  - **Example:**
    ```
    Switch(config-if)# power inline consumption 5000
    ```
  - Configures the power consumption of a powered device connected to a PoE port on the switch.
  - The range for each device is 4000 to 30000 mW (PoE+). The default is 30000 mW (PoE+).

Step 6
- **end**
  - **Example:**
    ```
    Switch(config-if)# end
    ```
  - Returns to privileged EXEC mode.

Step 7
- **show power inline consumption**
  - **Example:**
    ```
    Switch# show power inline consumption
    ```
  - Displays the power consumption data.

Step 8
- **copy running-config startup-config**
  - **Example:**
    ```
    Switch# copy running-config startup-config
    ```
  - (Optional) Saves your entries in the configuration file.

---

### Configuring Power Policing

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

**Note**
The power consumption is displayed in units of 0.5 W. For example, if a connected device draws 3.9 W, this feature will display 4.0 W power drawn.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4.  power inline police [action {log | errdisable}]
5.  exit
6.  Use one of the following:
   •  errdisable detect cause inline-power
   •  errdisable recovery cause inline-power
   •  errdisable recovery interval interval
7.  exit
8.  Use one of the following:
   •  show power inline police
   •  show errdisable recovery
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></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>interface interface-id</td>
<td>Specifies the physical port to be configured, and enter interface configuration mode.</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>
<tr>
<td>4</td>
<td>power inline police [action {log</td>
<td>errdisable}]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# power inline police</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  You can enable error detection for the PoE error-disabled cause by using the `errdisable detect cause inline-power` global configuration command. You can also enable the timer to recover from the PoE error-disabled state by using the `errdisable recovery cause inline-power interval interval` global configuration command.
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>power inline police action errdisable</strong>—Turns off power to the port if the real-time power consumption exceeds the maximum power allocation on the port.</td>
</tr>
<tr>
<td>• <strong>power inline police action log</strong>—Generates a syslog message while still providing power to the port.</td>
</tr>
<tr>
<td>If you do not enter the <strong>action log</strong> keywords, the default action shuts down the port and puts the port in the error-disabled state.</td>
</tr>
</tbody>
</table>

### Step 5

**exit**

**Example:**

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

Returns to global configuration mode.

### Step 6

**Use one of the following:**

- `errdisable detect cause inline-power`
- `errdisable recovery cause inline-power`
- `errdisable recovery interval interval`

**Example:**

```
Switch(config)# errdisable detect cause inline-power
Switch(config)# errdisable recovery cause inline-power
Switch(config)# errdisable recovery interval 100
```

(Optional) Enables error recovery from the PoE error-disabled state, and configures the PoE recovery mechanism variables.

By default, the recovery interval is 300 seconds.

For `interval interval`, specifies the time in seconds to recover from the error-disabled state. The range is 30 to 86400.

### Step 7

**exit**

**Example:**

```
Switch(config)# exit
```

Returns to privileged EXEC mode.

### Step 8

**Use one of the following:**

- `show power inline police`
- `show errdisable recovery`

**Example:**

```
Switch# show power inline police
Switch# show errdisable recovery
```

Displays the power monitoring status, and verify the error recovery settings.

### Step 9

**copy running-config startup-config**

**Example:**

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

(Optional) Saves your entries in the configuration file.
Monitoring Power Status

Table 11: Show Commands for Power Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show env power switch [switch-number]</td>
<td>(Optional) Displays the status of the internal power supplies for the specified switch.</td>
</tr>
<tr>
<td>show power inline [interface-id</td>
<td>module switch-number]</td>
</tr>
<tr>
<td>show power inline police</td>
<td>Displays the power policing data.</td>
</tr>
</tbody>
</table>

Note

Use the `debug ilpower controller` privileged EXEC command to enable debugging of the platform-specific Power over Ethernet (PoE) software module on the switch in long message format. These messages include the Power Controller register reading. Use the `no` form of this command to disable debugging.

Configuration Examples for Configuring PoE

Budgeting Power: Example

When you enter one of the following commands,

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

this caution message appears:

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

Default EEE Configuration

How to Configure EEE

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

Enabling or Disabling EEE

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><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>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>power efficient-ethernet auto</code> <strong>Example:</strong> <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>4</td>
<td><code>no power efficient-ethernet auto</code> <strong>Example:</strong> <code>Switch(config-if)# no power efficient-ethernet auto</code></td>
<td>Disables EEE on the specified interface.</td>
</tr>
<tr>
<td>5</td>
<td><code>end</code> <strong>Example:</strong> <code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td><code>copy running-config startup-config</code> <strong>Example:</strong> <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 12: 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>

Following are examples of the `show eee` commands:

```
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

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the 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 Configuring EEE

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

IP Multicast Snooping

• Configuring IGMP Snooping, on page 85
• Configuring MLD Snooping, on page 117
Configuring IGMP Snooping

• Finding Feature Information, on page 85
• Prerequisites for Configuring IGMP Snooping, on page 85
• Restrictions for Configuring IGMP Snooping, on page 86
• Information About IGMP Snooping, on page 87
• How to Configure IGMP Snooping, on page 92
• Monitoring IGMP Snooping, on page 110
• Configuration Examples for IGMP Snooping, on page 112
• Additional References, on page 114

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
Restrictions for Configuring IGMP Snooping

Restrictions for Configuring IGMP Snooping

The following are the restrictions for IGMP snooping:

- 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.
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:
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

Joining a Multicast Group

*Figure 2: Initial IGMP Join Message*

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 13: 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.
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 14: 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 Statickally to Join a Group
  - Example: Configuring a Host Statickally to Join a Group, on page 112

**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 97
- Example: Enabling IGMP Immediate Leave, on page 112

### 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 98

### 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.

**Related Topics**
- Disabling IGMP Report Suppression, on page 102
Default IGMP Snooping Configuration

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

Table 15: 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

Related Topics

- Enabling or Disabling IGMP Snooping on a Switch, on page 92
- Enabling or Disabling IGMP Snooping on a VLAN Interface, on page 93

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.

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

**Related Topics**
- Configuring IGMP Profiles, on page 103
- Applying IGMP Profiles, on page 106
- Setting the Maximum Number of IGMP Groups, on page 107
- Configuring the IGMP Throttling Action, on page 108
- Restrictions for IGMP Snooping

### Default IGMP Filtering and Throttling Configuration

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

<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><strong>Note</strong></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: 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> ip igmp snooping</td>
<td>Globally enables IGMP snooping in all existing VLAN interfaces.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip igmp snooping</td>
<td><strong>Note</strong> To globally disable IGMP snooping on all VLAN interfaces, use the <code>no ip igmp snooping</code> global configuration command.</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>
<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**

Default IGMP Snooping Configuration, on page 91

### Enabling or Disabling IGMP Snooping on a VLAN Interface

Follow these steps to enable 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>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>enable</code></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></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>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<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. <strong>Note</strong> To disable IGMP snooping on a VLAN interface, use the <code>no ip igmp snooping vlan vlan-id</code> global configuration command for the specified VLAN number.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>ip igmp snooping vlan 7</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></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>Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</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>Switch# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

## Related Topics

- Default IGMP Snooping Configuration, on page 91

### 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.
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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></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; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></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# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip igmp snooping vlan vlan-id mrouter interface interface-id</code></td>
<td>Specifies the multicast router VLAN ID and the interface to the multicast router.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ip igmp snooping vlan 5 mrouter interface gigabitethernet0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To remove a multicast router port from the VLAN, use the <code>no ip igmp snooping vlan vlan-id mrouter interface interface-id</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></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)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show ip igmp snooping mrouter [vlan vlan-id]</code></td>
<td>Verifies that IGMP snooping is enabled on the VLAN interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### 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 mac_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> 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> <code>ip igmp snooping vlan vlan-id static mac_address interface interface-id</code></td>
<td>Statically configures a Layer 2 port as a member of a multicast group:</td>
</tr>
<tr>
<td>Example:</td>
<td>• <code>vlan-id</code> is the multicast group VLAN ID. The range is 1 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>

---

**Related Topics**

Example: Enabling a Static Connection to a Multicast Router
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config)# ip igmp snooping vlan 105 static 0100.1212.0000 interface gigabitethernet0/1 | • mac-address is the group MAC address.  
• interface-id is the member port. It can be a physical interface or a port channel (1 to 6).  
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. |

### Step 4

**Example:**

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

- Returns to privileged EXEC mode.

### Step 5

**Example:**

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

- Verifies the member port and the IP address.

### Step 6

**Example:**

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

- (Optional) Saves your entries in the configuration file.

---

**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

---

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L 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></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> ip igmp snooping vlan <code>vlan-id</code> immediate-leave</td>
<td>Enables IGMP Immediate Leave on the VLAN interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip igmp snooping vlan 21 immediate-leave</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To disable IGMP Immediate Leave on a VLAN, use the no ip igmp snooping vlan <code>vlan-id</code> immediate-leave global configuration command.</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 ip igmp snooping vlan <code>vlan-id</code></td>
<td>Verifies that Immediate Leave is enabled on the VLAN interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip igmp snooping vlan 21</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>
</tbody>
</table>

### Related Topics
- [Immediate Leave](#), on page 89
- [Example: Enabling IGMP Immediate Leave](#), on page 112

### 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`
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>
</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)# ip igmp snooping last-member-query-interval 1000` | Configures the IGMP leave timer globally. The range is 100 to 32767 milliseconds.  
The default leave time is 1000 milliseconds.  
**Note** To globally reset the IGMP leave timer to the default setting, use the `no ip igmp snooping last-member-query-interval global` configuration command. |
| **Step 4**  
**Example:**  
`Switch(config)# ip igmp snooping vlan 210 last-member-query-interval 1000` | (Optional) Configures the IGMP leave time on the VLAN interface. The range is 100 to 32767 milliseconds.  
**Note** Configuring the leave time on a VLAN overrides the globally configured timer.  
**Note** To remove the configured IGMP leave-time setting from the specified VLAN, use the `no ip igmp snooping vlan vlan-id last-member-query-interval global` configuration command. |
| **Step 5**  
**Example:** | Returns to privileged EXEC mode. |
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: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

(Optional) Displays the configured IGMP leave time.

(Optional) Saves your entries in the configuration file.

Related Topics

IGMP Configurable-Leave Timer, on page 90
<table>
<thead>
<tr>
<th><strong>Step</strong></th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</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>3</td>
<td><code>ip igmp snooping querier</code></td>
<td>Enables the IGMP snooping querier.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip igmp snooping querier</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>ip igmp snooping querier address ip_address</code></td>
<td>(Optional) 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.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip igmp snooping querier address 172.16.24.1</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>ip igmp snooping querier query-interval interval-count</code></td>
<td>(Optional) Sets the interval between IGMP queriers. The range is 1 to 18000 seconds.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip igmp snooping querier query-interval 30</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`ip igmp snooping querier tcn query [count count</td>
<td>interval interval]`</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip igmp snooping querier tcn query interval 20</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<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></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip igmp snooping querier timer expiry 180</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<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></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip igmp snooping querier version 2</code></td>
<td></td>
</tr>
</tbody>
</table>
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>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>

---

**Related Topics**

IGMP Snooping, on page 87  
Prerequisites for IGMP Snooping, on page 85  
Example: Setting the IGMP Snooping Querier Source Address, on page 112  
Example: Setting the IGMP Snooping Querier Maximum Response Time, on page 113  
Example: Setting the IGMP Snooping Querier Timeout, on page 113  
Example: Setting the IGMP Snooping Querier Feature, on page 113
### 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>
</tbody>
</table>

### Step 2

**configure terminal**

**Example:**

```
Switch# configure terminal
```

### Step 3

**no ip igmp snooping report-suppression**

**Example:**

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

Disables IGMP report suppression. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers.

IGMP report suppression is enabled by default.

When IGMP report suppression is enabled, the switch forwards only one IGMP report per multicast router query.

**Note** 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 90

**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
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>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>Switch&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

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

| **Step 3** | 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: | • deny—Specifies that matching addresses are denied; this is the default. |
| Switch(config)# ip igmp profile 3 | • exit—Exits from igmp-profile configuration mode. |
| | • no—Negates a command or returns to its defaults. |
| | • permit—Specifies that matching addresses are permitted. |
| | • range—Specifies a range of IP addresses for the profile. You can enter a single IP address or a range with a start and an end address. |
| | The default is for the switch to have no IGMP profiles configured. |
| | **Note** To delete a profile, use the **no ip igmp profile profile number** global configuration command. |
### Configuring IGMP Profiles

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>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 <code>range</code> command multiple times to enter multiple addresses or ranges of addresses. <strong>Note</strong> To delete an IP multicast address or range of IP multicast addresses, use the <code>no range ip multicast address</code> IGMP profile configuration command.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Verifies the profile configuration.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

#### Related Topics
- IGMP Filtering and Throttling, on page 91
- Restrictions for IGMP Snooping
# 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></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></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>
</tbody>
</table>

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

| **Step 3** | interface interface-id |
| **Example:** | Switch(config)# interface gigabitethernet0/1 |
| | 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. |

| **Step 4** | ip igmp filter profile number |
| **Example:** | Switch(config-if)# ip igmp filter 321 |
| | Applies the specified IGMP profile to the interface. The range is 1 to 4294967295. |
| **Note** | To remove a profile from an interface, use the no ip igmp filter profile number interface configuration command. |

| **Step 5** | end |
| **Example:** | |
| | Returns to privileged EXEC mode. |
### 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>Step 1 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>
### 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Example: Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface interface-id</strong>&lt;br&gt;Example: Switch(config)# interface gigabitethernet0/2</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>ip igmp max-groups number</strong>&lt;br&gt;Example: Switch(config-if)# ip igmp max-groups 20</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong>&lt;br&gt;Example: Switch(config)# end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show running-config interface interface-id</strong>&lt;br&gt;Example: Switch# interface gigabitethernet0/1</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>copy running-config startup-config</strong>&lt;br&gt;Example: Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Related Topics
- IGMP Filtering and Throttling, on page 91
- Restrictions for IGMP Snooping
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`
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></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>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></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><code>Switch(config)# interface gigabitethernet0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`ip igmp max-groups action {deny</td>
<td>replace}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-if)# ip igmp max-groups action replace</code></td>
<td>• <strong>deny</strong>—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></td>
</tr>
<tr>
<td></td>
<td>• <strong>replace</strong>—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, this configuration causes the switch to replace the current group with the specified one.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</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>

**Note**  
To return to the default action of dropping the report, use the `no ip igmp max-groups action` interface configuration command.

**Step 5**  
`end`  
Example:  
`Switch(config)# end`

Returns to privileged EXEC mode.

**Step 6**  
`show running-config interface interface-id`  
Example:  
`Switch# show running-config interface gigabitethernet0/1`

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**  
- IGMP Filtering and Throttling, on page 91  
- Restrictions for IGMP Snooping

**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 17: Commands for Displaying IGMP Snooping Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `show ip igmp snooping [vlan vlan-id [detail]]` | Displays the snooping configuration information for all VLANs on the switch or for a specified VLAN.  
(Optional) Enter `vlan vlan-id` to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| `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 mrouter [vlan vlan-id]` | Displays information on dynamically learned and manually configured multicast router interfaces.  
**Note** When you enable IGMP snooping, the switch automatically learns the interface to which a multicast router is connected. These are dynamically learned interfaces.  
(Optional) Enter the `vlan vlan-id` to display information for a particular VLAN. |
| `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 18: Commands for Displaying IGMP Filtering

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip igmp profile [profile number]</code></td>
<td>Displays the specified IGMP profile or all the IGMP profiles defined on the switch.</td>
</tr>
<tr>
<td><code>show running-config [interface interface-id]</code></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: 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 interface gigabitethernet0/2
Switch end

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
 Joining a Multicast Group, on page 88

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 97
 Immediate Leave, on page 89

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:

Switch# configure terminal
Switch(config)# ip igmp snooping querier 10.0.0.64
Switch(config)# end

Related Topics
 Configuring the IGMP Snooping Querier, on page 100
 IGMP Snooping, on page 87
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

Related Topics
- Configuring the IGMP Snooping Querier, on page 100
- IGMP Snooping, on page 87

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

Related Topics
- Configuring the IGMP Snooping Querier, on page 100
- IGMP Snooping, on page 87

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

Related Topics
- Configuring the IGMP Snooping Querier, on page 100
- IGMP Snooping, on page 87

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

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

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:

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>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td></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><em>Host Extensions for IP Multicasting</em></td>
</tr>
<tr>
<td>RFC 2236</td>
<td><em>Internet Group Management Protocol, Version 2</em></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the 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>
CHAPTER 9

Configuring MLD Snooping

This module contains details of configuring MLD snooping

- Finding Feature Information, on page 117
- Information About Configuring IPv6 MLD Snooping, on page 117
- How to Configure IPv6 MLD Snooping, on page 120
- Displaying MLD Snooping Information, on page 127
- Configuration Examples for Configuring MLD Snooping, on page 128

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>
</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

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.

To globally enable MLD snooping on the switch, perform this procedure:

**Procedure**

<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> ipv6 mld snooping</td>
<td>Enables MLD snooping on the switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ipv6 mld 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) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> reload</td>
<td>Reload the operating system.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# reload</td>
<td></td>
</tr>
</tbody>
</table>
Enabling or Disabling MLD Snooping on a VLAN

To enable MLD snooping on a VLAN, perform this procedure:

**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>enable</code></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; <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>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ipv6 mld snooping</code></td>
<td>Enables MLD snooping on the switch.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ipv6 mld snooping</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ipv6 mld snooping vlan vlan-id</code></td>
<td>Enables MLD snooping on the VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Note: MLD snooping must be globally enabled for VLAN snooping to be enabled.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ipv6 mld snooping vlan 1</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>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>ipv6 mld snooping vlan 1</code></td>
<td></td>
</tr>
</tbody>
</table>

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>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></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Switch&gt; <code>enable</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&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

#### Step 2

**Example:**

```
Switch# configure terminal
```

#### Step 3

**ipv6 mld snooping vlan **

```
ipv6_mld_snooping_vlan vlan-id static
ipv6_multicast_address interface interface-id
```

**Example:**

```
Switch(config)# ipv6 mld snooping vlan 1 static
3333.0000.1111 interface gigabitethernet 0/1
```

- *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).

#### Step 4

**Example:**

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

#### Step 5

Use one of the following:

- `show ipv6 mld snooping address`
- `show ipv6 mld snooping address vlan vlan-id`

**Example:**

```
Switch# show ipv6 mld snooping address
or
Switch# show ipv6 mld snooping vlan 1
```

Verifies the static member port and the IPv6 address.

---

### Enabling MLD Immediate Leave

To enable MLDv1 immediate leave, perform this procedure:

#### Procedure

<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>
</tbody>
</table>

---

![Image]

IP Multicast Snooping
### Configuring MLD Snooping Queries

To configure MLD snooping query characteristics for the switch or for a VLAN, 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><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>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>ipv6 mld snooping vlan vlan-id immediate-leave</code></td>
<td>Enables MLD Immediate Leave on the VLAN interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ipv6 mld snooping vlan 1 immediate-leave</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></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></td>
</tr>
<tr>
<td><code>show ipv6 mld snooping vlan vlan-id</code></td>
<td>Verifies that Immediate Leave is enabled on the VLAN interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show ipv6 mld snooping vlan 1</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 ipv6 mld snooping vlan vlan-id robustness-variable value</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: Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 3</td>
<td></td>
</tr>
<tr>
<td>Step 5 ipv6 mld snooping last-listener-query-count count</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: Switch(config)# ipv6 mld snooping last-listener-query-count 7</td>
<td></td>
</tr>
<tr>
<td>Step 6 ipv6 mld snooping vlan vlan-id last-listener-query-count count</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: Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-count 7</td>
<td></td>
</tr>
<tr>
<td>Step 7 ipv6 mld snooping last-listener-query-interval interval</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: Switch(config)# ipv6 mld snooping last-listener-query-interval 2000</td>
<td></td>
</tr>
<tr>
<td>Step 8 ipv6 mld snooping vlan vlan-id last-listener-query-interval interval</td>
<td>(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.</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 2000</td>
<td></td>
</tr>
<tr>
<td>Step 9 ipv6 mld snooping tcn query solicit</td>
<td>(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.</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 mld snooping tcn query solicit</td>
<td></td>
</tr>
<tr>
<td>Step 10 ipv6 mld snooping tcn flood query count count</td>
<td>(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.</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 mld snooping tcn flood query count 5</td>
<td></td>
</tr>
<tr>
<td>Step 11 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 12 show ipv6 mld snooping querier [ vlan vlan-id]</td>
<td>(Optional) Verifies that the MLD snooping querier information for the switch or for the VLAN.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Disabling MLD Listener Message Suppression

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.

To disable MLD listener message suppression, 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><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</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>Enter 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></td>
</tr>
<tr>
<td><code>no ipv6 mld snooping listener-message-suppression</code></td>
<td>Disable MLD message suppression.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# no ipv6 mld snooping listener-message-suppression</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return 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></td>
</tr>
<tr>
<td><code>show ipv6 mld snooping</code></td>
<td>Verify that IPv6 MLD snooping report suppression is disabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show ipv6 mld snooping</code></td>
<td></td>
</tr>
</tbody>
</table>

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 20: Commands for Displaying MLD Snooping Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 mld snooping [ vlan vlan-id ]</code></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><code>show ipv6 mld snooping mrouter [ vlan vlan-id ]</code></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><code>show ipv6 mld snooping querier [ vlan vlan-id ]</code></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>
<tr>
<td>`show ipv6 mld snooping address [ count</td>
<td>vlan vlan-id ]`</td>
</tr>
<tr>
<td>• Enters <code>count</code> to show the group count on the switch or in a VLAN.</td>
<td></td>
</tr>
<tr>
<td>• Enters <code>user</code> to display MLD snooping user-configured group information for the switch or for a VLAN.</td>
<td></td>
</tr>
<tr>
<td><code>show ipv6 mld snooping address vlan vlan-id [ ipv6-multicast-address ]</code></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:

```bash
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet1/1
Switch(config)# end
```
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# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```
Configuring MLD Snooping Queries: Example
PART III

IPv6

• Configuring IPv6 Unicast Routing, on page 133
• Configuring IPv6 ACL, on page 147
CHAPTER 10

Configuring IPv6 Unicast Routing

• Finding Feature Information, on page 133
• Information About Configuring IPv6 Host Functions, on page 133
• Configuration Examples for IPv6 Unicast Routing, on page 145

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 Host Functions

This chapter describes how to configure IPv6 host functions on the Catalyst 2960L switch.

For information about configuring IPv6 Multicast Listener Discovery (MLD) snooping, see Configuring MLD Snooping.

Understanding IPv6

IPv4 users can move to IPv6 and receive services such as end-to-end security, quality of service (QoS), and globally unique addresses. The IPv6 address space reduces the need for private addresses and Network Address Translation (NAT) processing by border routers at network edges.


For information about IPv6 and other features in this chapter

• See the Cisco IOS IPv6 Configuration Library.
IPv6 Addresses

The switch supports only IPv6 unicast addresses. It does not support site-local unicast addresses, or anycast addresses.

The IPv6 128-bit addresses are represented as a series of eight 16-bit hexadecimal fields separated by colons in the format: n:n:n:n:n:n:n:n. This is an example of an IPv6 address:

2031:0000:130F:0000:0000:09C0:080F:130B

For easier implementation, leading zeros in each field are optional. This is the same address without leading zeros:

2031:0:130F:0:0:9C0:80F:130B

You can also use two colons (::) to represent successive hexadecimal fields of zeros, but you can use this short version only once in each address:

2031::0:130F:0:0:9C0:80F:130B


Supported IPv6 Unicast Routing Features

These sections describe the IPv6 protocol features supported by the switch:

128-Bit Wide Unicast Addresses

The switch supports aggregatable global unicast addresses and link-local unicast addresses. It does not support site-local unicast addresses.

• Aggregatable global unicast addresses are IPv6 addresses from the aggregatable global unicast prefix. The address structure enables strict aggregation of routing prefixes and limits the number of routing table entries in the global routing table. These addresses are used on links that are aggregated through organizations and eventually to the Internet service provider.

These addresses are defined by a global routing prefix, a subnet ID, and an interface ID. Current global unicast address allocation uses the range of addresses that start with binary value 001 (2000::/3). Addresses with a prefix of 2000::/3(001) through E000::/3(111) must have 64-bit interface identifiers in the extended unique identifier (EUI)-64 format.

• Link local unicast addresses can be automatically configured on any interface by using the link-local prefix FE80::/10(1111 1110 10) and the interface identifier in the modified EUI format. Link-local addresses are used in the neighbor discovery protocol (NDP) and the stateless autoconfiguration process. Nodes on a local link use link-local addresses and do not require globally unique addresses to communicate. IPv6 routers do not forward packets with link-local source or destination addresses to other links.

For more information, see the section about IPv6 unicast addresses in the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.
IPv6 supports Domain Name System (DNS) record types in the DNS name-to-address and address-to-name lookup processes. The DNS AAAA resource record types support IPv6 addresses and are equivalent to an A address record in IPv4. The switch supports DNS resolution for IPv4 and IPv6.

**ICMPv6**

The Internet Control Message Protocol (ICMP) in IPv6 generates error messages, such as ICMP destination unreachable messages, to report errors during processing and other diagnostic functions. In IPv6, ICMP packets are also used in the neighbor discovery protocol and path MTU discovery.

**Neighbor Discovery**

The switch supports NDP for IPv6, a protocol running on top of ICMPv6, and static neighbor entries for IPv6 stations that do not support NDP. The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), to verify the reachability of the neighbor, and to keep track of neighboring routers.

The switch supports ICMPv6 redirect for routes with mask lengths less than 64 bits. ICMP redirect is not supported for host routes or for summarized routes with mask lengths greater than 64 bits.

Neighbor discovery throttling ensures that the switch CPU is not unnecessarily burdened while it is in the process of obtaining the next hop forwarding information to route an IPv6 packet. The switch drops any additional IPv6 packets whose next hop is the same neighbor that the switch is actively trying to resolve. This drop avoids further load on the CPU.

---

**Note**

All IPv6 Next Hop Security are not supported in Cisco IOS Release 15.2(5)E.

**IPv6 Stateless Autoconfiguration and Duplicate Address Detection**

The switch uses stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses. A host autonomously configures its own link-local address, and booting nodes send router solicitations to request router advertisements for configuring interfaces.

For more information about autoconfiguration and duplicate address detection, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of *Cisco IOS IPv6 Configuration Library* on Cisco.com.

**IPv6 Applications**

The switch has IPv6 support for these applications:

- Ping, traceroute, and Telnet
- Secure Shell (SSH) over an IPv6 transport
- HTTP server access over IPv6 transport
- DNS resolver for AAAA over IPv4 transport
- Cisco Discovery Protocol (CDP) support for IPv6 addresses

For more information about managing these applications, see the *Cisco IOS IPv6 Configuration Library* on Cisco.com.
Static Routes for IPv6

Static routes are manually configured and define an explicit route between two networking devices. Static routes are useful for smaller networks with only one path to an outside network or to provide security for certain types of traffic in a larger network.

Configuring Static Routing for IPv6 (CLI)

For configuring static routes for IPv6, see the Configuring Static Routing for IPv6 section.

For more information about static routes, see the “Implementing Static Routes for IPv6” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.

RIP for IPv6

Routing Information Protocol (RIP) for IPv6 is a distance-vector protocol that uses hop count as a routing metric. It includes support for IPv6 addresses and prefixes and the all-RIP-routers multicast group address FF02::9 as the destination address for RIP update messages.

For configuring RIP for IPv6, see the Configuring RIP for IPv6 section.

For more information about RIP for IPv6, see the “Implementing RIP for IPv6” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.

SNMP and Syslog Over IPv6

To support both IPv4 and IPv6, IPv6 network management requires both IPv6 and IPv4 transports. Syslog over IPv6 supports address data types for these transports.

Simple Network Management Protocol (SNMP) and syslog over IPv6 provide these features:

• Support for both IPv4 and IPv6
• IPv6 transport for SNMP and to modify the SNMP agent to support traps for an IPv6 host
• SNMP- and syslog-related MIBs to support IPv6 addressing
• Configuration of IPv6 hosts as trap receivers

For support over IPv6, SNMP modifies the existing IP transport mapping to simultaneously support IPv4 and IPv6. These SNMP actions support IPv6 transport management:

• Opens User Datagram Protocol (UDP) SNMP socket with default settings
• Provides a new transport mechanism called SR_IPV6_TRANSPORT
• Sends SNMP notifications over IPv6 transport
• Supports SNMP-named access lists for IPv6 transport
• Supports SNMP proxy forwarding using IPv6 transport
• Verifies SNMP Manager feature works with IPv6 transport

For information on SNMP over IPv6, including configuration procedures, see the “Managing Cisco IOS Applications over IPv6” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.

For information about syslog over IPv6, including configuration procedures, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.
HTTP(S) Over IPv6

The HTTP client sends requests to both IPv4 and IPv6 HTTP servers, which respond to requests from both IPv4 and IPv6 HTTP clients. URLs with literal IPv6 addresses must be specified in hexadecimal using 16-bit values between colons.

The accept socket call chooses an IPv4 or IPv6 address family. The accept socket is either an IPv4 or IPv6 socket. The listening socket continues to listen for both IPv4 and IPv6 signals that indicate a connection. The IPv6 listening socket is bound to an IPv6 wildcard address.

The underlying TCP/IP stack supports a dual-stack environment. HTTP relies on the TCP/IP stack and the sockets for processing network-layer interactions.

Basic network connectivity (ping) must exist between the client and the server hosts before HTTP connections can be made.

For more information, see the “Managing Cisco IOS Applications over IPv6” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.

Default IPv6 Configuration

Table 21: Default IPv6 Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 addresses</td>
<td>None configured</td>
</tr>
</tbody>
</table>

Configuring IPv6 Addressing and Enabling IPv6 Routing

This section describes how to assign IPv6 addresses to individual Layer 3 interfaces and to globally forward IPv6 traffic on the switch.

Before configuring IPv6 on the switch, consider the following:

- In the ipv6 address interface configuration command, you must enter the ipv6-address and ipv6-prefix variables with the address specified in hexadecimal using 16-bit values between colons. The prefix-length variable (preceded by a slash [/]) is a decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

To forward IPv6 traffic on an interface, you must configure a global IPv6 address on that interface. Configuring an IPv6 address on an interface automatically configures a link-local address and activates IPv6 for the interface. The configured interface automatically joins these required multicast groups for that link:

- solicited-node multicast group FF02:0:0:0:1::/104 for each unicast address assigned to the interface (this address is used in the neighbor discovery process.)
- all-nodes link-local multicast group FF02::1
- all-routers link-local multicast group FF02::2

For more information about configuring IPv6 routing, see the “Implementing Addressing and Basic Connectivity for IPv6” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.

Beginning in privileged EXEC mode, follow these steps to assign an IPv6 address to a Layer 3 interface and enable IPv6 forwarding:
**SUMMARY STEPS**

1. configure terminal
2. end
3. reload
4. configure terminal
5. interface interface-id
6. Use one of the following:
   - ipv6 address ipv6-prefix/prefix length eui-64
   - ipv6 address ipv6-address/prefix length
   - ipv6 address ipv6-address link-local
   - ipv6 enable
7. exit
8. end
9. show ipv6 interface interface-id
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> 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> 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 3</strong> reload</td>
<td>Reloads the operating system.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# reload</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> configure terminal</td>
<td>Enters global configuration mode after the switch reloads.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface interface-id</td>
<td>Enters interface configuration mode, and specifies the Layer 3 interface to configure.</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(config)# interface gigabitethernet0/1</td>
<td>Specifies a global IPv6 address with an extended unique identifier (EUI) in the low-order 64 bits of the IPv6 address. Specify only the network prefix; the last 64 bits are automatically computed from the switch MAC address. This enables IPv6 processing on the interface.</td>
</tr>
</tbody>
</table>

**Step 6**

Use one of the following:

- `ipv6 address ipv6-prefix/prefix length eui-64`
- `ipv6 address ipv6-address/prefix length`
- `ipv6 address ipv6-address link-local`
- `ipv6 enable`

**Example:**

Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64

Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64

Switch(config-if)# ipv6 address FE80::/10 link-local

Switch(config-if)# ipv6 enable

- Manually configures an IPv6 address on the interface.
- Specifies a link-local address on the interface to be used instead of the link-local address that is automatically configured when IPv6 is enabled on the interface. This command enables IPv6 processing on the interface.
- Automatically configures an IPv6 link-local address on the interface, and enables the interface for IPv6 processing. The link-local address can only be used to communicate with nodes on the same link.

**Step 7**

`exit`

**Example:**

Switch(config-if)# exit

Returns to global configuration mode.

**Step 8**

`end`

**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

**Step 9**

`show ipv6 interface interface-id`

**Example:**

Switch# show ipv6 interface gigabitethernet0/1

Verifies your entries.

**Step 10**

`copy running-config startup-config`

**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.
# Configuring IPv6 ICMP Rate Limiting

ICMP rate limiting is enabled by default with a default interval between error messages of 100 milliseconds and a bucket size (maximum number of tokens to be stored in a bucket) of 10.

To change the ICMP rate-limiting parameters, perform this procedure:

## 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>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Switch&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>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ipv6 icmp error-interval interval [bucketsize]</code></td>
<td>Configures the interval and bucket size for IPv6 ICMP error messages:</td>
</tr>
<tr>
<td>Example:</td>
<td><code>ipv6 icmp error-interval 50 20</code></td>
<td>• <code>interval</code>—The interval (in milliseconds) between tokens being added to the bucket. The range is from 0 to 2147483647 milliseconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>bucketsize</code>—(Optional) The maximum number of tokens stored in the bucket. The range is from 1 to 200.</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>end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show ipv6 interface [interface-id]</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>show ipv6 interface gigabitethernet0/1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show ipv6 interface gigabitethernet0/1</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<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><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
# Configuring Static Routing for IPv6 (CLI)

Before configuring a static IPv6 route, you must enable routing by using the `ip routing` global configuration command, enable the forwarding of IPv6 packets by using the `ipv6 unicast-routing` global configuration command, and enable IPv6 on at least one Layer 3 interface by configuring an IPv6 address on the interface.

**Note**

The switch supports 16 IPv6 static routes.

For more information about configuring static IPv6 routing, see the “Implementing Static Routes for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

## Procedure

<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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** | Configures a static IPv6 route. |
| `ipv6 route ipv6-prefix/prefix length {ipv6-address | interface-id [ipv6-address]} [administrative distance]` | |
| **Example:** | |
| Switch(config)# `ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130` | |

- `ipv6-prefix` — The IPv6 network that is the destination of the static route. It can also be a hostname when static host routes are configured.

- `/prefix length` — The length of the IPv6 prefix. A decimal value that shows how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

- `ipv6-address` — The IPv6 address of the next hop that can be used to reach the specified network. The IPv6 address of the next hop need not be directly connected; recursion is done to find the IPv6 address of the directly connected next hop. The address must be in the form documented in RFC 2373, specified in hexadecimal using 16-bit values between colons.

- `interface-id` — Specifies direct static routes from point-to-point and broadcast interfaces. With point-to-point interfaces, there is no need to specify the IPv6 address of the next hop. With broadcast interfaces, you should always specify the IPv6 address of the next hop, or ensure that the specified prefix is assigned to the link, specifying a link-local address as the next hop. You can optionally specify the IPv6 address of the next hop to which packets are sent.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note</strong> You must specify an <em>interface-id</em> when using a link-local address as the next hop (the link-local next hop must also be an adjacent router).</td>
</tr>
<tr>
<td></td>
<td>• <em>administrative distance</em>—(Optional) An administrative distance. The range is 1 to 254; the default value is 1, which gives static routes precedence over any other type of route except connected routes. To configure a floating static route, use an administrative distance greater than that of the dynamic routing protocol.</td>
</tr>
</tbody>
</table>

**Step 3**

**Example:**

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

Returns to privileged EXEC mode.

**Step 4**

Use one of the following:

- **show ipv6 static** `[ipv6-address | ipv6-prefix/prefix length] [interface interface-id] [detail] [recursive]`
- **show ipv6 route static**

**Example:**

```
Switch# show ipv6 static 2001:0DB8::/32 interface gigabitethernet0/1
```

or

```
Switch# show ipv6 route static
```

Verifies your entries by displaying the contents of the IPv6 routing table.

- **interface interface-id**—(Optional) Displays only those static routes with the specified interface as an egress interface.
- **recursive**—(Optional) Displays only recursive static routes. The recursive keyword is mutually exclusive with the interface keyword, but it can be used with or without the IPv6 prefix included in the command syntax.
- **detail**—(Optional) Displays this additional information:
  - For valid recursive routes, the output path set, and maximum resolution depth.
  - For invalid routes, the reason why the route is not valid.

**Step 5**

**copy running-config startup-config**

**Example:**

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

(Optional) Saves your entries in the configuration file.

---

**Configuring RIP for IPv6**

For more information about configuring RIP routing for IPv6, see the “Implementing RIP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com,
To configure RIP routing for IPv6, perform this procedure:

**Before you begin**

Before configuring the switch to run IPv6 RIP, you must enable routing by using the `ip routing` global configuration command, enable the forwarding of IPv6 packets by using the `ipv6 unicast-routing` global configuration command, and enable IPv6 on any Layer 3 interfaces on which IPv6 RIP is to be enabled.

**Procedure**

<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. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch&gt; enable</code></td>
<td></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>ipv6 router rip name</code></td>
<td>Configures an IPv6 RIP routing process, and enters router configuration mode for the process.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# ipv6 router rip cisco</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>maximum-paths number-paths</code></td>
<td>(Optional) Define the maximum number of equal-cost routes that IPv6 RIP can support. The range is from 1 to 8, and the default is 8 routes.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-router)# maximum-paths 6</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-router)# exit</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>interface interface-id</code></td>
<td>Enters interface configuration mode, and specifies the Layer 3 interface to configure.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>ipv6 rip name enable</code></td>
<td>Enables the specified IPv6 RIP routing process on the interface.</td>
</tr>
</tbody>
</table>
### Configuring RIP for IPv6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config-if)# ipv6 rip cisco enable</code></td>
<td>(Optional) Enables IPv6 RIP on the switch.</td>
</tr>
</tbody>
</table>

**Step 8**

- `ipv6 rip name default-information {only | originate}`

  **Example:**
  ```
  Switch(config-if)# ipv6 rip cisco default-information only
  ```

  (Optional) Originates the IPv6 default route (::/0) into the RIP routing process updates sent from the specified interface.

  **Note**  
  To avoid routing loops after the IPv6 default route (::/0) is originated from any interface, the routing process ignores all default routes received on any interface.

  - **only**—Select to originate the default route, but suppress all other routes in the updates sent on this interface.
  - **originate**—Select to originate the default route in addition to all other routes in the updates sent on this interface.

**Step 9**

- `end`

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

  Returns to privileged EXEC mode.

**Step 10**

- Use one of the following:
  - `show ipv6 rip [name] [ interface interface-id] [ database ] [ next-hops ]`
  - `show ipv6 rip`

  **Example:**
  ```
  Switch# show ipv6 rip cisco interface gigabitethernet 0/1
  or
  Switch# show ipv6 rip
  ```

  - Displays information about current IPv6 RIP processes.
  - Displays the current contents of the IPv6 routing table.

**Step 11**

- `copy running-config startup-config`

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

  (Optional) Saves your entries in the configuration file.
### Displaying IPv6

For complete syntax and usage information on these commands, see the Cisco IOS command reference publications.

**Table 22: Command for Monitoring IPv6**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 access-list</td>
<td>Displays a summary of access lists.</td>
</tr>
<tr>
<td>show ipv6 cef</td>
<td>Displays Cisco Express Forwarding for IPv6.</td>
</tr>
<tr>
<td>show ipv6 interface interface-id</td>
<td>Displays IPv6 interface status and configuration.</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>Displays IPv6 neighbor cache entries.</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>Displays a list of IPv6 prefix lists.</td>
</tr>
<tr>
<td>show ipv6 protocols</td>
<td>Displays a list of IPv6 routing protocols on the switch.</td>
</tr>
<tr>
<td>show ipv6 rip</td>
<td>Displays IPv6 RIP routing protocol status.</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Displays IPv6 route table entries.</td>
</tr>
<tr>
<td>show ipv6 static</td>
<td>Displays IPv6 static routes.</td>
</tr>
<tr>
<td>show ipv6 traffic</td>
<td>Displays IPv6 traffic statistics.</td>
</tr>
</tbody>
</table>

### Configuration Examples for IPv6 Unicast Routing

#### Configuring IPv6 Addressing and Enabling IPv6 Routing: Example

This example shows how to enable IPv6 with both a link-local address and a global address based on the IPv6 prefix 2001:0DB8:c18:1::/64. The EUI-64 interface ID is used in the low-order 64 bits of both addresses. Output from the `show ipv6 interface` EXEC command is included to show how the interface ID (20B:46FF:FE2F:D940) is appended to the link-local prefix FE80::/64 of the interface.

```
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet0/11
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet0/11
GigabitEthernet0/11 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF2F:D940
MTU is 1500 bytes
```
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

Configuring IPv6 ICMP Rate Limiting: Example

This example shows how to configure an IPv6 ICMP error message interval of 50 milliseconds and a bucket size of 20 tokens.

```
Switch(config)#ipv6 icmp error-interval 50 20
```

Configuring Static Routing for IPv6: Example

This example shows how to configure a floating static route to an interface with an administrative distance of 130:

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet 0/1 130
```

Displaying IPv6: Example

This is an example of the output from the `show ipv6 interface` privileged EXEC command:

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
Global unicast address(es):
  3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF2F:D940
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
<output truncated>
```
CHAPTER 11

Configuring IPv6 ACL

- Finding Feature Information, on page 147
- Information About Configuring IPv6 ACLs, on page 147
- Configuring IPv6 ACLs, on page 148
- Configuration Examples for IPv6 ACL, on page 154

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.

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><strong>Step 1</strong></td>
<td>Create an IPv6 ACL, and enter IPv6 access list configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure the IPv6 ACL to block (deny) or pass (permit) traffic.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Apply the IPv6 ACL to an interface.</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 use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 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, 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><strong>Example:</strong></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Define an IPv6 access list name, and enter IPv6 access-list configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>ipv6 access-list access-list-name</code></td>
</tr>
<tr>
<td><code>ipv6 access-list access-list-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>- 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.</td>
</tr>
<tr>
<td>`{deny</td>
<td>permit} protocol`</td>
</tr>
<tr>
<td>`{deny</td>
<td>permit} protocol `</td>
</tr>
<tr>
<td>`{source-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
<tr>
<td><code>[operator [port-number]]</code></td>
<td>- (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.</td>
</tr>
<tr>
<td>`[destination-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</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 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>
</tbody>
</table>

### Step 5

**Example:**

```
{deny | permit} tcp
{source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address}
{operator [port-number]}{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address}
{operator [port-number]}{ack | dscp value} {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 3, with these additional optional parameters:

- **ack**—Acknowledgment bit set.
- **fin**—Finished bit set; no more data from sender.
- **neq** {port | protocol}—Matches only packets that are not on a given port number.
- **psh**—Push function bit set.
- **range** {port | protocol}—Matches only packets in the port number range.
- **rst**—Reset bit set.
- **syn**—Synchronize bit set.
- **urg**—Urgent pointer bit set.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Define a UDP access list and the access conditions.</td>
</tr>
<tr>
<td>{deny|permit} udp</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>{deny | permit} udp (\text{source-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Define an ICMP access list and the access conditions.</td>
</tr>
<tr>
<td>{deny|permit} icmp</td>
<td>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:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>{deny | permit} icmp (\text{source-ipv6-prefix/prefix-length</td>
<td>any</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td>(\text{Switch(config)}# \text{end})</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Verify the access list configuration.</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>(\text{show ipv6 access-list})</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>show running-config</td>
<td>(\text{Switch}# \text{show running-config})</td>
</tr>
</tbody>
</table>
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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal Example: Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface interface_id Example: Switch# 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><strong>Step 3</strong> ipv6 traffic-filter access-list-name Example: Switch# ipv6 traffic-filter access-list-name in</td>
<td>Apply the access list to incoming or outgoing traffic on the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end Example: Switch(config)# end</td>
<td>Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Verify the access list configuration.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config Example: copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Displaying IPv6 ACLs

To display IPv6 ACLs, perform this procedure:
### Procedure

<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> show access-list</td>
<td>Displays all access lists configured on the switch</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show access-lists</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> show ipv6 access-list</td>
<td>Displays all configured IPv6 access list or the access list specified by name.</td>
</tr>
<tr>
<td>acl_name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# show ipv6 access-list [access-list-name]</td>
<td></td>
</tr>
</tbody>
</table>

### Configuration Examples for IPv6 ACL

#### Example: Creating an 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.

```
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.

```plaintext
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 159
- Configuring Multiple Spanning-Tree Protocol, on page 185
- Configuring Optional Spanning-Tree Features, on page 229
- Configuring Resilient Ethernet Protocol, on page 261
- Configuring EtherChannels, on page 279
- Configuring Link-State Tracking, on page 307
- Configuring UniDirectional Link Detection, on page 313
CHAPTER 12

Configuring Spanning Tree Protocol

This chapter describes how to configure the Spanning Tree Protocol (STP) on port-based VLANs on the Catalyst switches. The switch can use either the per-VLAN spanning-tree plus (PVST+) protocol based on the IEEE 802.1D standard and Cisco proprietary extensions, or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol based on the IEEE 802.1w standard. A switch stack appears as a single spanning-tree node to the rest of the network, and all stack members use the same bridge ID.

- Finding Feature Information, on page 159
- Restrictions for STP, on page 159
- Information About Spanning Tree Protocol, on page 160
- How to Configure Spanning-Tree Features, on page 170
- Monitoring Spanning-Tree Status, on page 183

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.

Related Topics
- Configuring the Root Switch, on page 173
- Bridge ID, Device Priority, and Extended System ID, on page 162
- Spanning-Tree Topology and BPDUs, on page 161
- Accelerated Aging to Retain Connectivity, on page 167

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.
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.

**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,

- 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.

- 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.

**Note**

If the *logging event spanning tree* command is configured on multiple interfaces and the topology changes, it may result in several logging messages and high CPU utilization. This may cause the switch to drop or delay the processing of STP BPDUs.

To prevent this behavior, remove the *logging event spanning tree* and *logging event status* commands or disable logging to the console.

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 173
[Restrictions for STP](#), on page 159

### 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>
<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 Bit 14 Bit 13 Bit 12 Bit 11 Bit 10 Bit 9 Bit 8 Bit 7 Bit 6 Bit 5 Bit 4 Bit 3 Bit 2 Bit 1</td>
</tr>
<tr>
<td>32768</td>
<td>16384 8192 4096 2048 1024 512 256 128 64 32 16 8 4 2 1</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.

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 173
- Restrictions for STP, on page 159
- Configuring the Root Switch, on page 206
- Root Switch, on page 188
- Specifying the MST Region Configuration and Enabling MSTP, on page 204

**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 175
- Configuring Path Cost, on page 177

**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 4: 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 BPDU 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
Layer 2

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
- Discards frames switched from another interface for forwarding
- Learns addresses
- Receives BPDUs

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
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 5: 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 175

Spanning Tree and Redundant Connectivity

Figure 6: 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 173
- Restrictions for STP, on page 159

**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 re provision 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 172
- Default Spanning-Tree Configuration, on page 170
- Default MSTP Configuration, on page 200

**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 24: 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 204
- MSTP Configuration Guidelines, on page 187
- Multiple Spanning-Tree Regions, on page 188

**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 25: 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>
<tr>
<td>Spanning-tree port cost (configurable on a per-interface basis)</td>
<td>1000 Mb/s: 4&lt;br&gt;100 Mb/s: 19&lt;br&gt;10 Mb/s: 100</td>
</tr>
<tr>
<td>Spanning-tree VLAN port priority (configurable on a per-VLAN basis)</td>
<td>128</td>
</tr>
<tr>
<td>Spanning-tree VLAN port cost (configurable on a per-VLAN basis)</td>
<td>1000 Mb/s: 4&lt;br&gt;100 Mb/s: 19&lt;br&gt;10 Mb/s: 100</td>
</tr>
<tr>
<td>Spanning-tree timers</td>
<td>Hello time: 2 seconds&lt;br&gt;Forward-delay time: 15 seconds&lt;br&gt;Maximum-aging time: 20 seconds&lt;br&gt;Transmit hold count: 6 BPDUs</td>
</tr>
</tbody>
</table>

**Note**

Beginning in Cisco IOS Release 15.2(4)E, the default STP mode is Rapid PVST+.

**Related Topics**

- [Disabling Spanning Tree](#), on page 172
- [Supported Spanning-Tree Instances](#), on page 168

**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> 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> spanning-tree mode {pvst</td>
<td>mst</td>
</tr>
<tr>
<td>Example:</td>
<td>All stack members run the same version of spanning tree.</td>
</tr>
<tr>
<td>Switch(config)# spanning-tree mode pvst</td>
<td>• Select <strong>pvst</strong> to enable PVST+.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>mst</strong> to enable MSTP.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>rapid-pvst</strong> 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>Switch(config)# interface FastEthernet1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> spanning-tree link-type point-to-point</td>
<td>Specifies that the link type for this port is point-to-point. 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>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree link-type point-to-point</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>
</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 `vlan-id`
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>
</tbody>
</table>

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

| Step 3 no spanning-tree vlan `vlan-id` | For `vlan-id`, the range is 1 to 4094. |
| Example: Switch(config)` no spanning-tree vlan 300 | |
**Configuring the Root Switch**

To configure a switch as the root for the specified VLAN, use the `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 `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 `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>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></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### 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]`
### Configuring Port Priority

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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `enable`          | Enables privileged EXEC mode.  
  Example:  
  Switch> `enable`  
  • Enter your password if prompted. |
| 2    | `configure terminal` | Enters global configuration mode.  
  Example:  
  Switch# `configure terminal` |
| 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` |
| 4    | `spanning-tree port-priority priority` | Configures the port priority for an interface.  
  For `priority`, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.  
  Example:  
  Switch(config-if)# `spanning-tree port-priority 0` |
| 5    | `spanning-tree vlan vlan-id port-priority priority` | Configures the port priority for a VLAN.  
  • 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.  
  • For `priority`, the range is 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.  
  Example:  
  Switch(config-if)# `spanning-tree vlan 20-25 port-priority 0` |
| 6    | `end`             | Returns to privileged EXEC mode.  
  Example:  
  Switch(config-if)# `end` |

### Related Topics

- Port Priority Versus Path Cost, on page 163
- How a Switch or Port Becomes the Root Switch or Root Port, on page 166
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><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. Valid interfaces include physical ports and port-channel logical interfaces (port-channel port-channel-number).</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 4</strong> spanning-tree cost cost</td>
<td>Configures the cost for an interface.</td>
</tr>
<tr>
<td>Example:</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>Switch(config-if)# spanning-tree cost 250</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> spanning-tree vlan vlan-id cost cost</td>
<td>Configures the cost for a VLAN.</td>
</tr>
<tr>
<td>Example:</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 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>Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300</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 163

### 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.

**Note**

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>
<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></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>Configures the switch priority of a VLAN.</td>
</tr>
</tbody>
</table>

**Step 3**

**Configure the switch priority of a VLAN.**

```plaintext
Example:
Switch(config)# spanning-tree vlan 20 priority 8192
```

- 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.
- 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.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></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.

**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>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>
</tbody>
</table>

| Step 2(spanning-tree vlan `vlan-id hello-time seconds`) | Configures the hello time of a VLAN. The hello time is the time interval between configuration messages generated |
| Example: | |
### Purpose

Command or Action

Switch(config)# spanning-tree vlan 20-24 hello-time 3

Switch(config)# spanning-tree vlan 20,25 forward-time 18

**Purpose**

and sent by the root switch. These messages mean that the switch is alive.

- 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.
- For `seconds`, the range is 1 to 10; the default is 2.

### Example:

#### Step 3

**end**

**Example:**

Switch(config-if)# end

### 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><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></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# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>spanning-tree vlan <code>vlan-id forward-time seconds</code></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></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# spanning-tree vlan 20,25 forward-time 18</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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong></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><strong>configure terminal</strong></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><strong>spanning-tree vlan vlan-id max-age seconds</strong></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></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# spanning-tree vlan 20 max-age 30</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>
</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 transmit hold-count *value* | 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.  
  Example:  
  Switch(config)# spanning-tree transmit hold-count 6 |
### Monitoring Spanning-Tree Status

**Table 26: Commands for Displaying Spanning-Tree Status**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show spanning-tree active</code></td>
<td>Displays spanning-tree information on active interfaces only.</td>
</tr>
<tr>
<td><code>show spanning-tree detail</code></td>
<td>Displays a detailed summary of interface information.</td>
</tr>
<tr>
<td><code>show spanning-tree vlan vlan-id</code></td>
<td>Displays spanning-tree information for the specified VLAN.</td>
</tr>
<tr>
<td><code>show spanning-tree interface interface-id</code></td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td><code>show spanning-tree interface interface-id portfast</code></td>
<td>Displays spanning-tree portfast information for the specified interface.</td>
</tr>
<tr>
<td><code>show spanning-tree summary [totals]</code></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.
Monitoring Spanning-Tree Status
CHAPTER 13

Configuring Multiple Spanning-Tree Protocol

- Finding Feature Information, on page 185
- Prerequisites for MSTP, on page 185
- Restrictions for MSTP, on page 186
- Information About MSTP, on page 187
- How to Configure MSTP Features, on page 204
- Examples, on page 222
- Monitoring MST Configuration and Status, on page 226
- Feature Information for MSTP, on page 227

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 27: 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 204
- MSTP Configuration Guidelines, on page 187
- Multiple Spanning-Tree Regions, on page 188
- Configuring the Root Switch, on page 206
- Root Switch, on page 188
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).

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 206
- Restrictions for MSTP, on page 186
- Bridge ID, Device Priority, and Extended System ID, on page 162

**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 191
- Specifying the MST Region Configuration and Enabling MSTP, on page 204
- Prerequisites for MSTP, on page 185
- Restrictions for MSTP, on page 186
- Spanning-Tree Interoperability and Backward Compatibility, on page 168
- Optional Spanning-Tree Configuration Guidelines
- BackboneFast, on page 233
- UplinkFast, on page 231

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 191

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 BPU 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 191

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 28: 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.
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's 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 8: 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 changes.

---

**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.
Figure 9: Detecting Unidirectional Link Failure

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 BPDUs 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 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 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 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 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 BPDUs as if they are RSTP BPDUs. Therefore, MSTP switches send either a Version 0 configuration and TCN BPDUs or Version 3 MSTP BPDUs 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 29: Port State Comparison**

<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.

  **Figure 10: Proposal and Agreement Handshaking for Rapid Convergence**

Switch A is connected to Switch B through a point-to-point link, and all of the ports are in the blocking state. Assume that the priority of Switch A is a smaller numerical value than the priority of Switch B.
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.

**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 11: 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 30: 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>
</tbody>
</table>
**Function Bit**

<table>
<thead>
<tr>
<th>Bit</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<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 BPDUs.

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 BPDUs 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 nonedge ports except on those from which it received the TC notification.

- **Notification**—Unlike IEEE 802.1D, which uses TCN BPDUs, the RSTP does not use them. However, for IEEE 802.1D interoperability, an RSTP switch processes and generates TCN BPDUs.
• 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 219

### 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>
### 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:

```plaintext
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) bpdus filter: disable (default)
  Boundary : boundary (PVST) bpdus guard : disable (default)
  Bpdus sent 10, received 310
```

---

<table>
<thead>
<tr>
<th><strong>Feature</strong></th>
<th><strong>Default Setting</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning-tree port priority (configurable on a per-CIST port basis)</td>
<td>128</td>
</tr>
<tr>
<td>Spanning-tree port cost (configurable on a per-CIST port basis)</td>
<td></td>
</tr>
<tr>
<td>1000 Mb/s: 20000</td>
<td></td>
</tr>
<tr>
<td>100 Mb/s: 20000</td>
<td></td>
</tr>
<tr>
<td>10 Mb/s: 20000</td>
<td></td>
</tr>
<tr>
<td>Hello time</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Forward-delay time</td>
<td>20 seconds</td>
</tr>
<tr>
<td>Maximum-aging time</td>
<td>20 seconds</td>
</tr>
<tr>
<td>Maximum hop count</td>
<td>20 hops</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Specifying the MST Region Configuration and Enabling MSTP](https://www.cisco.com/c/en/us/support/docs/catalyst-switches/15-204.html), on page 204
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 12: 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 13: Loss of Connectivity*

[Diagram showing loss of connectivity between A and R]

- 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 14: 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>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>
</tbody>
</table>

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

| **Step 3** spanning-tree mst configuration | Enters MST configuration mode.                                         |
| Example:                                 |                                                                         |
| Switch(config)# spanning-tree mst configuration |                                                             |

| **Step 4** instance instance-id vlan vlan-range | Maps VLANs to an MST instance.                                      |

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
### Specifying the MST Region Configuration and Enabling MSTP

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-mst)# instance 1 vlan 10-20</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>name <code>name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-mst)# name region1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>revision <code>version</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-mst)# revision 1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show pending</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-mst)# show pending</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-mst)# exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>spanning-tree mode mst</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# spanning-tree mode mst</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
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>
</tbody>
</table>

Related Topics

MSTP Configuration Guidelines, on page 187
Multiple Spanning-Tree Regions, on page 188
Prerequisites for MSTP, on page 185
Restrictions for MSTP, on page 186
Spanning-Tree Interoperability and Backward Compatibility, on page 168
Optional Spanning-Tree Configuration Guidelines
BackboneFast, on page 233
UplinkFast, on page 231
Default MSTP Configuration, on page 200
Configuring the Root Switch, on page 206
Bridge ID, Device Priority, and Extended System ID, on page 162
Configuring a Secondary Root Switch, on page 207
Configuring Port Priority, on page 208
Configuring Path Cost, on page 210
Configuring the Switch Priority, on page 211
Configuring the Hello Time, on page 213
Configuring the Forwarding-Delay Time, on page 214
Configuring the Maximum-Aging Time, on page 215
Configuring the Maximum-Hop Count, on page 216
Specifying the Link Type to Ensure Rapid Transitions, on page 217
Designating the Neighbor Type, on page 218
Restarting the Protocol Migration Process, on page 219
### 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.

---

**Table: Command or Action and Purpose**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>spanning-tree mst instance-id root primary</code></td>
<td>Configures a switch as the root switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# spanning-tree mst 0 root primary</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></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>
</tbody>
</table>

**Related Topics**

- [Root Switch](#)
- [Specifying the MST Region Configuration and Enabling MSTP](#)
- [Restrictions for MSTP](#)
- [Bridge ID, Device Priority, and Extended System ID](#)
- [Configuring a Secondary Root Switch](#)

---

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
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: 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 mst instance-id root secondary</td>
<td>Configures a switch as the secondary root switch.</td>
</tr>
<tr>
<td>Example: Switch(config)# spanning-tree mst 0 root secondary</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><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>

**Related Topics**

- Specifying the MST Region Configuration and Enabling MSTP, on page 204
- Configuring the Root Switch, on page 206

### 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>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>Example: Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></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></td>
<td>Example: Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface interface-id</code></td>
<td>Specifies an interface to configure, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>spanning-tree mst instance-id port-priority priority</code></td>
<td>Configures port priority.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-if)# <code>spanning-tree mst 0 port-priority 64</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></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></td>
<td></td>
<td>• For <em>priority</em>, the range is 0 to 240 in increments of 16. The default is 128. The lower the number, the higher the priority.</td>
</tr>
</tbody>
</table>
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.

**Step 5**

**Example:**

```
Switch(config-if)# end
```

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 204
- Configuring Path Cost, on page 210

**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><strong>Step 1</strong></td>
<td>enable</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>
<tr>
<td><strong>Step 2</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>
<tr>
<td><strong>Step 3</strong></td>
<td>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.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the cost.</td>
</tr>
<tr>
<td>spanning-tree mst instance-id cost cost</td>
<td>Confirms 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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree mst 0 cost 17031970</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 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 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

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 208
- Specifying the MST Region Configuration and Enabling MSTP, on page 204

**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; 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> spanning-tree mst instance-id priority priority</td>
<td>Configures the switch priority.</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>• For <code>priority</code>, the range is 0 to 61440 in increments of 4096; the</td>
</tr>
<tr>
<td></td>
<td>default is 32768. The lower the number, the more likely the switch</td>
</tr>
<tr>
<td></td>
<td>will be chosen as the root switch.</td>
</tr>
<tr>
<td>Switch(config)# spanning-tree mst 0 priority 40960</td>
<td></td>
</tr>
</tbody>
</table>
Priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. These are the only acceptable values.

Step 4

Example:
Switch(config-if)# end

Returns to privileged EXEC mode.

Related Topics
Specifying the MST Region Configuration and Enabling MSTP, on page 204

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

Step 1

Command or Action
enable

Example:
Switch> enable

Purpose
Enables privileged EXEC mode.

Step 2

Command or Action
configure terminal

Example:
Switch# configure terminal

Purpose
Enters global configuration mode.
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>• 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> 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>
<tr>
<td>Example:</td>
<td></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>
</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 max-age seconds`
  
  **Example:**
  
  `Switch(config)# spanning-tree mst max-age 40`
| 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. |
### 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> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <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: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>spanning-tree mst max-hops hop-count</code></td>
<td>Specifies the number of hops in a region before the BPDU 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: <code>Switch(config)# spanning-tree mst max-hops 25</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Specifying the MST Region Configuration and Enabling MSTP, on page 204
Related Topics
Specifying the MST Region Configuration and Enabling MSTP, on page 204

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>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>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th>configure terminal</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>interface interface-id</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>spanning-tree link-type point-to-point</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example: Switch(config-if)# spanning-tree link-type point-to-point</td>
<td>Specifies that the link type of a port is point-to-point.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example: Switch(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Related Topics

- Specifying the MST Region Configuration and Enabling MSTP, on page 204

### 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>
<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></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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specifies an interface to configure,</td>
</tr>
<tr>
<td>Example:</td>
<td>and enters interface configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> spanning-tree mst pre-standard</td>
<td>Specifies that the port can send only</td>
</tr>
<tr>
<td>Example:</td>
<td>prestandard BPDUs.</td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree mst pre-standard</td>
<td></td>
</tr>
<tr>
<td></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

Specifying the MST Region Configuration and Enabling MSTP, on page 204

### 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 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 Enter one of the following commands:
   • clear spanning-tree detected-protocols
   • clear spanning-tree detected-protocols interface interface-id

Example:
Switch# clear spanning-tree detected-protocols
or
Switch# clear spanning-tree detected-protocols interface gigabitethernet 0/1

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 204
Protocol Migration Process, on page 200

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>
<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>spanning-tree mst simulate pvst global</td>
<td>Enables PVST+ simulation globally.</td>
</tr>
<tr>
<td>Example:</td>
<td>To prevent the switch from automatically interoperating with a connecting switch that is running Rapid PVST+, enter the no version of the command.</td>
</tr>
<tr>
<td>Switch(config)# spanning-tree mst simulate pvst global</td>
<td></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>
</tbody>
</table>

**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>
<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>
</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)# interface0/1
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 0/1 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
  ---------------- ---- --- --------- -------- -------------------------
  Gi0/1 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
Name Blocking Listening Learning Forwarding STP Active
------------------------ -------- --------- -------- ---------- ----------
MST0 2 0 0 0 0 2
------------------------ -------- --------- -------- ---------- ----------
1 mst 2 0 0 0 0 2

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
Name Blocking Listening Learning Forwarding STP Active
------------------------ -------- --------- -------- ---------- ----------
MST0 2 0 0 0 0 2
------------------------ -------- --------- -------- ---------- ----------
1 mst 2 0 0 0 0 2

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
Portfast BPDU Filter Default is disabled
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>
<tr>
<td>3 vlans</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>

This example shows the interface details when PVST+ simulation is globally enabled, or the default configuration:

Switch# show spanning-tree interface0/1 detail
Port 269 (GigabitEthernet0/1) 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 interface0/1 detail
Port 269 (GigabitEthernet0/1) 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 interface0/1 detail
Port 269 (GigabitEthernet0/1) 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 interface0/1 detail
Port 269 (GigabitEthernet0/1) 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 0/1 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
  --------------  ----  ---  ---------  --------  -------------------------
  Gi0/1  Desg  BKN  4  128.270  P2p  Dispute

This example shows the interface details when a dispute condition is detected:

Switch# show spanning-tree interface0/1 detail
Port 269 (GigabitEthernet0/1) 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 32: Commands for Displaying MST Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree mst configuration</td>
<td>Displays the MST region configuration.</td>
</tr>
<tr>
<td>show spanning-tree mst configuration digest</td>
<td>Displays the MD5 digest included in the current MSTCI.</td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| `show spanning-tree mst` | Displays MST information for the all instances.  
  **Note**  This command displays information for ports in a link-up operative state. |
| `show spanning-tree mst instance-id` | Displays MST information for the specified instance.  
  **Note**  This command displays information only if the port is in a link-up operative state. |
| `show spanning-tree mst interface interface-id` | Displays MST information for the specified interface. |

## Feature Information for MSTP

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 14

Configuring Optional Spanning-Tree Features

• Finding Feature Information, on page 229
• Restriction for Optional Spanning-Tree Features, on page 229
• Information About Optional Spanning-Tree Features, on page 230
• How to Configure Optional Spanning-Tree Features, on page 240
• Examples, on page 256
• Monitoring the Spanning-Tree Status, on page 259
• Feature Information for Optional Spanning-Tree Features, on page 259

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 240
PortFast, on page 230
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 15: 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 240
- Restriction for Optional Spanning-Tree Features, on page 229

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 242

## 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 BPDU. The interfaces still send a few BPDU at link-up before the switch begins to filter outbound BPDU. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDU. 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 BPDU.

---

**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 243

## UplinkFast

**Figure 16: 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 loops.

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.
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.

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 204
- MSTP Configuration Guidelines, on page 187
- Multiple Spanning-Tree Regions, on page 188
- Enabling UplinkFast for Use with Redundant Links, on page 244
- 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 BPDDUs 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 19: 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 20: 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 21: Adding a Switch in a Shared-Medium Topology

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 204
- MSTP Configuration Guidelines, on page 187
- Multiple Spanning-Tree Regions, on page 188
- Enabling BackboneFast, on page 247

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 248

### Root Guard

*Figure 22: 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.

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]`.

**Note**

**Related Topics**

- Enabling PortFast Port Types, on page 251

## 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.

**Note**

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 23: 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.

**Figure 25: Network with STP Topology Running Bridge Assurance**

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.

**Figure 26: Network Problem Averted with Bridge Assurance Enabled**

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:
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 255

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>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>Switch&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>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies an interface to configure, and enters interface configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td></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></td>
<td>Enables PortFast on an access port connected to a single workstation or server.</td>
</tr>
<tr>
<td>spanning-tree portfast {disable</td>
<td>edge</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter the following keywords for additional options:</td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree portfast edge</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Enter disable to disable portfast for the interface.</td>
</tr>
<tr>
<td></td>
<td>- Enter edge to enable portfast edge for the interface.</td>
</tr>
<tr>
<td></td>
<td>- Enter network to enable portfast network for the interface.</td>
</tr>
<tr>
<td></td>
<td>By default, PortFast is disabled on all interfaces.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></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

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 230
- [Restriction for Optional Spanning-Tree Features](#), on page 229

---

### 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>
</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)# interface gigabitethernet 0/2`
| Specifies the interface connected to an end station, and enters interface configuration mode. |
| **Step 4**
  
  Example: |
<p>| Enables the PortFast edge feature. |</p>
<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>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Example:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# end</td>
<td>Returns to privileged EXEC mode.</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 it in the error-disabled state.

**Related Topics**

- [BPDU Guard](#), on page 230

**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
### 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** | `spanning-tree portfast edge bpdufilter default` | Globally enables BPDU filtering.  
*Example:*  
`Switch(config)# spanning-tree portfast edge bpdufilter default`  
By default, BPDU filtering is disabled. |
| **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 231

### 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>
</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 uplinkfast [max-update-rate pkts-per-second] | Enables UplinkFast.  
  (Optional) For `pkts-per-second`, 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.  
  Example:  
  Switch(config)# `spanning-tree uplinkfast max-update-rate 200` |
| **Step 4** end | Returns to privileged EXEC mode.  
  Example:  
  Switch(config)# `end` |

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 231
  - 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> enable</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><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><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> no spanning-tree uplinkfast</td>
<td>Disables UplinkFast and CSUF on the switch and all of its VLANs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# no spanning-tree uplinkfast</code></td>
<td></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 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>
<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> 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></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><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> spanning-tree etherchannel guard misconfig</td>
<td>Enables EtherChannel guard.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- [BackboneFast](#), on page 233
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# spanning-tree etherchannel guard misconfig</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**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 235

**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
### 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>
<tbody>
<tr>
<td>1</td>
<td>show spanning-tree active</td>
<td>Verifies which interfaces are alternate or root ports.</td>
</tr>
<tr>
<td></td>
<td>show spanning-tree mst</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>spanning-tree loopguard default</td>
<td>Enables loop guard.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

Switch# show spanning-tree active
or
Switch# show spanning-tree mst

**Example:**

Switch(config)# spanning-tree loopguard default

**Example:**

Switch(config)# end

---

**Related Topics**

- **Loop Guard**, on page 237

---

### Enabling PortFast Port Types

This section describes the different steps to enable Portfast Port types.

**Related Topics**

- **STP PortFast Port Types**, on page 237
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> 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** spanning-tree portfast [edge | network | normal] default | Configures the default state for all interfaces on the switch. You have these options: |
| Example:                  | • (Optional) edge—Configures all interfaces as edge ports. This assumes all ports are connected to hosts/servers. |
| Switch(config)# spanning-tree portfast default | • (Optional) network—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. |
|                          | • (Optional) normal—Configures all interfaces normal spanning tree ports. These ports can be connected to any type of device. |
|                          | • default—The default port type is normal. |

| **Step 4** end | Returns to privileged EXEC mode. |
| Example: | Switch(config)# end |
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>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>interface interface-id</td>
<td>Specifies an interface to configure.</td>
</tr>
<tr>
<td>port-channel port_channel_number</td>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
</tr>
<tr>
<td>Step 4</td>
<td>spanning-tree portfast edge</td>
<td>Enables edge behavior on a Layer 2 access port connected to an end workstation or server.</td>
</tr>
<tr>
<td>[trunk]</td>
<td>Example:</td>
<td>• (Optional) trunk—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></td>
<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>
</table>
| **Step 1**        | **enable**  
**Example:**  
`Switch> enable` | Enables privileged EXEC mode.  
- Enter your password if prompted. |
<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>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>interface interface-id</td>
<td>Specifies an interface to configure.</td>
</tr>
<tr>
<td></td>
<td>port-channel port_channel_number</td>
<td></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>
<tr>
<td></td>
<td>port-channel port_channel_number</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>spanning-tree portfast network</td>
<td>Enables edge behavior on a Layer 2 access port connected to an end workstation or server.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# spanning-tree portfast network</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Exits configuration 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>6</td>
<td>show running interface interface-id</td>
<td>Verifies the configuration.</td>
</tr>
<tr>
<td></td>
<td>port-channel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port_channel_number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>port-channel port_channel_number</td>
<td></td>
</tr>
</tbody>
</table>

### 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>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>
</tbody>
</table>

| **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:**      | Bridge Assurance is enabled by default. |
| `Switch(config)# spanning-tree bridge assurance` | Use the `no` version of the command to disable the feature. |
| **Example:**      | Disabling Bridge Assurance causes all configured network ports to behave as normal spanning tree ports. |
| `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 238

## Examples

### Examples: Configuring PortFast Edge on a Specified Interface

This example shows how to enable edge behavior on GigabitEthernet interface 0/1:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
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 gigabitethernet0/1
Building configuration...
Current configuration:
!
interface GigabitEthernet0/1
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 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
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 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 0/1 as a network port:

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
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 gigabitethernet0/1
Building configuration...
Current configuration:
!
interface GigabitEthernet0/1
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
Example: Configuring Bridge Assurance

This output shows port GigabitEthernet 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
----------------- ---- --- --------- -------- ---------------------------------------
G10/0/1 Desg FWD 4 128.1  P2p Edge
Po4  Desg FWD 3 128.480 P2p Network
G14/0/1 Desg FWD 4 128.169 P2p Edge
G14/0/47  Desg FWD 4 128.215 P2p Network

The example shows the output for show spanning-tree summary.

Switch# show 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
Configured Pathcost method used is short
### Monitoring the Spanning-Tree Status

**Table 33: 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 interface-id</td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td>show spanning-tree mst interface interface-id</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 interface-id 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 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 15

Configuring Resilient Ethernet Protocol

• Finding Feature Information, on page 261
• Overview of Resilient Ethernet Protocol, on page 261
• How to Configure Resilient Ethernet Protocol, on page 266
• Monitoring Resilient Ethernet Protocol Configuration, on page 274
• Configuration Examples for Resilient Ethernet Protocol, on page 276
• Additional References for REP, on page 277
• Feature Information for Resilient Ethernet Protocol, on page 278

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.

Overview of Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) is a Cisco-proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A device can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Trunk Ethernet Flow Point (EFP) interfaces.

The following figure shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all the ports are operational (as in the segment on the left), a
single port is blocked, as shown by the diagonal line. When there is a failure in the network, the blocked port returns to the forwarding state to minimize network disruption.

*Figure 27: REP Open Segment*

The segment shown in the figure above is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All the hosts connected to devices inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure occurs on any segment or on any port on a REP segment, REP unblocks all the ports to ensure that connectivity is available through the other gateway.

The segment shown in the following figure is a ring segment, with both the edge ports located on the same device. With this configuration, you can create a redundant connection between any two devices in the segment.

*Figure 28: REP Ring Segment*

REP segments have the following characteristics:

- If all the ports in a segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN. If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, and cause a link failure, all the ports forward traffic on all the VLANs to ensure connectivity.
- In case of a link failure, alternate ports are unblocked as quickly as possible. When the failed link is up, a logically blocked port per VLAN is selected with minimal disruption to the network.

You can construct almost any type of network based on REP segments. REP also supports VLAN load balancing, which is controlled by the primary edge port (any port in the segment).
In access ring-topologies, the neighboring switch might not support REP as shown in the following figure. In this scenario, you can configure the non-REP-facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all the properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this scenario, the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

**Figure 29: Edge No-Neighbor Ports**

REP has these limitations:

- You must configure each segment port; an incorrect configuration might cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

**Link Integrity**

REP does not use an end-to-end polling function between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All the VLANs are blocked on an interface until the neighbor is detected. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- A neighbor does not acknowledge a local port as a peer.
Each port creates an adjacency with its immediate neighbor. After the neighbor adjacencies are created, the ports negotiate with each other to determine the blocked port for the segment, which will function as the alternate port. All the other ports become unblocked. By default, REP packets are sent to a bridge protocol data unit-class MAC address. The packets can also be sent to a Cisco multicast address, which is used only to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are dropped by the devices not running REP.

**Fast Convergence**

REP runs on a physical link basis and not on a per-VLAN basis. Only one hello message is required for all the VLANs, and this reduces the load on the protocol. We recommend that you create VLANs consistently on all the switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the entire network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring an administrative VLAN for the entire domain or for a particular segment.

**VLAN Load Balancing**

One edge port in the REP segment acts as the primary edge port; and another as the secondary edge port. It is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all the other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port in one of three ways:

- By entering the port ID of the interface. To identify the port ID of a port in the segment, enter the `show interface rep detail` interface configuration command for the port.

- By entering the `preferred` keyword to select the port that you previously configured as the preferred alternate port with the `rep segment segment-id preferred` interface configuration command.

- By entering the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is −256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers indicate the secondary edge port (offset number -1) and its downstream neighbors.

  **Note** Configure offset numbers on the primary edge port by identifying a port’s downstream position from the primary (or secondary) edge port. Never enter an offset value of 1 because that is the offset number of the primary edge port.

The following figure shows neighbor offset numbers for a segment, where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside of the ring show the offset numbers from the secondary edge port. Note that you can identify all the ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position from the secondary edge port). If E2 became the primary edge port, its offset number would then be 1 and E1 would be -1.
When the REP segment is complete, all the VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways:

- Manually trigger VLAN load balancing at any time by entering the `rep preempt segment segment-id` privileged EXEC command on the switch that has the primary edge port.

- Configure a preempt delay time by entering the `rep preempt delay seconds` interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends out a message to alert all the interfaces in the segment about the preemption. When the secondary port receives the message, the message is sent to the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all the VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load-balancing configuration.

Reconfigure the primary edge port to reconfigure load balancing. When you change the load-balancing configuration, the primary edge port waits for the `rep preempt segment` command or for the configured preempt delay period after a port failure and recovery, before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load-balancing status does not change. Configuring a new edge port might cause a new topology configuration.

**Spanning Tree Interaction**

REP does not interact with the STP or the Flex Link feature, but can coexist with both. A port that belongs to a segment is removed from spanning tree control, and STP BPDU is not accepted or sent from segment ports. Therefore, STP cannot run on a segment.

To migrate from an STP ring configuration to an REP segment configuration, begin by configuring a single port in the ring as part of the segment and continue by configuring contiguous ports to minimize the number of segments. Since each segment always contains a blocked port, multiple segments means multiple blocked
ports and a potential loss of connectivity. After the segment is configured in both directions up to the location of the edge ports, configure the edge ports.

**REP Ports**

REP segments consist of Failed, Open, or Alternate ports:

- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port transitions to alternate port state, blocking all the VLANs on the interface. Blocked-port negotiations occur, and when the segment settles, one blocked port remains in the alternate role and all the other ports become open ports.
- When a failure occurs in a link, all the ports move to the Failed state. When the Alternate port receives the failure notification, it changes to the Open state, forwarding all the VLANs.

A regular segment port converted to an edge port, or an edge port converted to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according to the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

**How to Configure Resilient Ethernet Protocol**

A segment is a collection of ports connected to one another in a chain and configured with a segment ID. To configure REP segments, configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment, using interface configuration mode. You should configure two edge ports in a segment, with one of them being the primary edge port and the other the secondary edge port by default. A segment should have only one primary edge port. If you configure two ports in a segment as primary edge ports, for example, ports on different switches, the REP selects one of them to serve as the segment's primary edge port. If required, you can configure the location to which segment topology change notices (STCNs) and VLAN load balancing are to be sent.

**Default REP Configuration**

REP is disabled on all the interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the task of sending segment topology change notices (STCNs) is disabled, all the VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all the VLANs in the primary edge port.

**REP Configuration Guidelines**

Follow these guidelines when configuring REP:
• We recommend that you begin by configuring one port and then configure contiguous ports to minimize the number of segments and the number of blocked ports.

• If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. In the `show rep interface` command output, the Port Role for this port is displayed as **Fail Logical Open**; the Port Role for the other failed port is displayed as **Fail No Ext Neighbor**. When the external neighbors for the failed ports are configured, the ports go through the alternate port transitions and eventually go to an open state, or remain as the alternate port, based on the alternate port selection mechanism.

• **REP** ports must be Layer 2 IEEE 802.1Q or Trunk ports.

• We recommend that you configure all the trunk ports in a segment with the same set of allowed VLANs.

• Be careful when configuring REP through a Telnet connection because REP blocks all the VLANs until another REP interface sends a message to unblock it. You might lose connectivity to the router if you enable REP in a Telnet session that accesses the router through the same interface.

• You cannot run REP and STP or REP and Flex Links on the same segment or interface.

• If you connect an STP network to an REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge might cause a bridging loop because STP does not run on REP segments. All the STP BPDUs are dropped at REP interfaces.

• You must configure all the trunk ports in a segment with the same set of allowed VLANs. If this is not done, misconfiguration occurs.

• If REP is enabled on two ports on a switch, both the ports must be either regular segment ports or edge ports. REP ports follow these rules:
  - There is no limit to the number of REP ports on a switch. However, only two ports on a switch can belong to the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must both be edge ports, regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
  - If two ports on a switch belong to the same segment, and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

• REP interfaces come up in a blocked state and remain in a blocked state until they are safe to be unblocked. You must, therefore, be aware of the status of REP interfaces to avoid sudden connection losses.

• REP sends all the LSL PDUs in the untagged frames to the native VLAN. The BPA message sent to a Cisco multicast address is sent to the administration VLAN, which is VLAN 1 by default.

• You can configure the duration for which a REP interface remains up without receiving a hello from a neighbor. Use the `rep lsl-age-timer` value interface configuration command to set the time from 120 ms to 10000 ms. The LSL hello timer is then set to the age-timer value divided by 3. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and checks for hello messages.
  - EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.
• REP ports cannot be configured as one of the following port types:
  • Switched Port Analyzer (SPAN) destination port
  • Tunnel port
  • Access port

• REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.
• There can be a maximum of 64 REP segments per switch.

Configuring REP Administrative VLAN

To avoid the delay created by link-failure messages, and VLAN-blocking notifications during load balancing, REP floods packets to a regular multicast address at the hardware flood layer (HFL). These messages are flooded to the whole network, and not just the REP segment. You can control the flooding of these messages by configuring an administrative VLAN.

Follow these guidelines when configuring the REP administrative VLAN:

• If you do not configure an administrative VLAN, the default is VLAN 1.
• You can configure one admin VLAN on the switch for all segments.
• The administrative VLAN cannot be the RSPAN VLAN.

To configure the REP administrative VLAN, follow these steps, beginning in privileged EXEC mode:

**SUMMARY STEPS**

1. configure terminal
2. rep admin vlan vlan-id
3. end
4. show interface [interface-id] rep detail
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>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>rep admin vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# rep admin vlan 2</td>
</tr>
<tr>
<td></td>
<td>Specifies the administrative VLAN. The range is from 2 to 4094.</td>
</tr>
<tr>
<td></td>
<td>To set the admin VLAN to 1, which is the default, enter the <strong>no rep admin vlan</strong> global configuration command.</td>
</tr>
</tbody>
</table>
Configuring a REP Interface

To configure REP, enable REP on each segment interface and identify the segment ID. This task is mandatory, and must be done before other REP configurations. You must also configure a primary and secondary edge port on each segment. All the other steps are optional.

Follow these steps to enable and configure REP on an interface:

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. switchport mode trunk
5. rep segment segment-id [edge [no-neighbor] [primary]] [preferred]
6. rep stcn {interface interface-id | segment id-list | stp}
7. rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}
8. rep preempt delay seconds
9. rep isl-age-timer value
10. end
11. show interface [interface-id] rep [detail]
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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</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 interface [interface-id] rep detail</td>
<td>(Optional) Verifies the configuration on a REP interface.</td>
</tr>
<tr>
<td>Example: Switch# show interface gigabitethernet1/1 rep detail</td>
<td></td>
</tr>
</tbody>
</table>

<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 switch startup configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup config</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a REP Interface

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface).</td>
</tr>
<tr>
<td>interface interface-id</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# interface gigabitethernet1/1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the interface as a Layer 2 trunk port.</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# switchport mode trunk</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enables REP on the interface and identifies a segment number. The segment ID range is from 1 to 1024.</td>
</tr>
<tr>
<td>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# rep segment 1 edge no-neighbor primary</td>
</tr>
</tbody>
</table>

**Note** You must configure two edge ports, including one primary edge port, for each segment.

These optional keywords are available:

- (Optional) **edge**—Configures the port as an edge port. Each segment has only two edge ports. Entering the keyword `edge` without the keyword `primary` configures the port as the secondary edge port.
- (Optional) **primary**—Configures the port as the primary edge port, the port on which you can configure VLAN load balancing.
- (Optional) **no-neighbor**—Configures a port with no external REP neighbors as an edge port. The port inherits all the properties of an edge port, and you can configure the properties the same way you would for an edge port.

**Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the keyword `primary` on both the switches, the configuration is valid. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the `show rep topology` privileged EXEC command.

- (Optional) **preferred**—Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port.</td>
<td><strong>Note</strong></td>
</tr>
</tbody>
</table>

### Step 6

rep stcn {interface interface-id | segment id-list | stp}  

**Example:**

```
Switch# rep stcn segment 25-50
```

(Optional) Configures the edge port to send segment topology change notices (STCNs).

- **interface interface-id**—Designates a physical interface or port channel to receive STCNs.
- **segment id-list**—Identifies one or more segments to receive STCNs. The range is from 1 to 1024.
- **stp**—Sends STCNs to STP networks.

**Note**  Spanning Tree (MST) mode is required on edge no-neighbor nodes when `rep stcn stp` command is configured for sending STCNs to STP networks.

### Step 7

rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}  

**Example:**

```
Switch# rep block port id 0009001818D68700 vlan 1-100
```

(Optional) Configures VLAN load balancing on the primary edge port, identifies the REP alternate port in one of three ways (`id port-id`, `neighbor_offset`, `preferred`), and configures the VLANs to be blocked on the alternate port.

- **id port-id**—Identifies the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the `show interface type number rep [detail]` privileged EXEC command.

- **neighbor_offset**—Number to identify the alternate port as a downstream neighbor from an edge port. The range is from -256 to 256, with negative numbers indicating the downstream neighbor from the secondary edge port. A value of 0 is invalid. Enter `-1` to identify the secondary edge port as the alternate port.

**Note**  Because you enter the `rep block port` command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port.

- **preferred**—Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.

- **vlanvlan-list**—Blocks one VLAN or a range of VLANs.
## Configuring a REP Interface

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• vlan all</strong></td>
<td>Blocks all the VLANs.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Enter this command only on the REP primary edge port.</td>
</tr>
</tbody>
</table>

### Step 8

**rep preempt delay seconds**

**Example:**

```
Switch# rep preempt delay 100
```

(Optional) Configures a preempt time delay.

- Use this command if you want VLAN load balancing to be automatically triggered after a link failure and recovery.
- The time delay range is between 15 to 300 seconds. The default is manual preemption with no time delay.

**Note** Enter this command only on the REP primary edge port.

### Step 9

**rep lsl-age-timer value**

**Example:**

```
Switch# rep lsl-age-timer 2000
```

(Optional) Configures a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor.

The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).

**Note**
- EtherChannel port channel interfaces do not support LSL age-timer values that are less than 1000 ms.
- Both the ports on the link should have the same LSL age configured in order to avoid link flaps.

### Step 10

**end**

**Example:**

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

Exits global configuration mode and returns to privileged EXEC mode.

### Step 11

**show interface [interface-id] rep [detail]**

**Example:**

```
Switch(config)# show interface gigabitethernet1/1 rep detail
```

(Optional) Displays the REP interface configuration.

### Step 12

**copy running-config startup-config**

**Example:**

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

(Optional) Saves your entries in the router startup configuration file.
Setting Manual Preemption for VLAN Load Balancing

If you do not enter the `rep preempt delay seconds` interface configuration command on the primary edge port to configure a preemption time delay, the default is to manually trigger VLAN load balancing on the segment. Be sure that all the other segment configurations have been completed before manually preempting VLAN load balancing. When you enter the `rep preempt delay segment segment-id` command, a confirmation message is displayed before the command is executed because preemption might cause network disruption.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. `rep preempt segment segment-id`
4. `show rep topology segment segment-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> 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> <code>rep preempt segment segment-id</code></td>
<td>Manually triggers VLAN load balancing on the segment.</td>
</tr>
<tr>
<td>Example:</td>
<td>You need to confirm the command before it is executed.</td>
</tr>
<tr>
<td>Switch# <code>rep preempt segment 100</code></td>
<td></td>
</tr>
<tr>
<td>The command will cause a momentary traffic disruption.</td>
<td></td>
</tr>
<tr>
<td>Do you still want to continue? [confirm]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>show rep topology segment segment-id</code></td>
<td>(Optional) Displays REP topology information.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <code>show rep topology segment 100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# end</td>
<td></td>
</tr>
</tbody>
</table>
Configuring SNMP Traps for REP

You can configure a router to send REP-specific traps to notify the Simple Network Management Protocol (SNMP) server of link-operational status changes and port role changes.

**SUMMARY STEPS**

1. configure terminal
2. snmp mib rep trap-rate value
3. end
4. show running-config
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> snmp mib rep trap-rate value</td>
<td>Enables the switch to send REP traps, and sets the number of traps sent per second.</td>
</tr>
<tr>
<td>Example: Switch(config)# snmp mib rep trap-rate 500</td>
<td>• Enter the number of traps sent per second. The range is from 0 to 1000. The default is 0 (no limit is imposed; a trap is sent at every occurrence).</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 running-config</td>
<td>(Optional) Displays the running configuration, which can be used to verify the REP trap configuration.</td>
</tr>
<tr>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config startup-config</td>
<td>(Optional) Saves your entries in the switch startup configuration file.</td>
</tr>
<tr>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Monitoring Resilient Ethernet Protocol Configuration**

You can display the rep interface and rep topology details using the commands in this topic.

* `show interface [interface-id] rep [detail]`
Displays REP configuration and status for an interface or for all the interfaces.

- (Optional) **detail**—Displays interface-specific REP information.

**Example:**

```bash
Device# show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

- **show rep topology [segment segment-id] [archive] [detail]**

Displays REP topology information for a segment or for all the segments, including the primary and secondary edge ports in the segment.

- (Optional) **archive**—Displays the last stable topology.

**Note**

An archive topology is not retained when the switch reloaded.

- (Optional) **detail**—Displays detailed archived information.

**Example:**

```bash
Device# show rep topology

REP Segment 1
BridgeName PortName Edge Role
----------------- ------ ---- ----
10.64.106.63 Te5/4 Pri Open
10.64.106.228 Te3/4 Open
10.64.106.228 Te3/3 Open
10.64.106.67 Te4/3 Open
10.64.106.67 Te4/4 Alt
10.64.106.63 Te4/4 Sec Open

REP Segment 3
BridgeName PortName Edge Role
----------------- ------ ---- ----
10.64.106.63 Gi50/1 Pri Open
```
Configuration Examples for Resilient Ethernet Protocol

This section provides the following configuration examples:

Example: Configuring the REP Administrative VLAN

This example shows how to configure the administrative VLAN as VLAN 100, and verify the configuration by entering the `show interface rep detail` command on one of the REP interfaces:

```
Switch# configure terminal
Switch(config)# rep admin vlan 100
Switch(config)# end
Switch# show interface gigabitethernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

The following example shows how to create an administrative VLAN per segment. Here, VLAN 2 is configured as the administrative VLAN only for REP segment 2. All the remaining segments that are not configured have VLAN 1 as the administrative VLAN by default.

```
Switch# configure terminal
Switch(config)# rep admin vlan 2 segment 2
Switch(config)# end
```

Example: Configuring a REP Interface

This example shows how to configure an interface as the primary edge port for segment 1, to send STCNs to segments 2 through 5, and to configure the alternate port as the port with port ID 0009001818D68700 to block...
all the VLANs after a preemption delay of 60 seconds after a segment port failure and recovery. The interface
is configured to remain up for 6000 ms without receiving a hello from a neighbor.

Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end

This example shows how to configure the same configuration when the interface has no external REP neighbor:

Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge no-neighbor primary
Switch (conf-if)# rep stcn segment 2-5
Switch (conf-if)# rep block port 0009001818D68700 vlan all
Switch (conf-if)# rep preempt delay 60
Switch (conf-if)# rep lsl-age-timer 6000
Switch (conf-if)# end

This example shows how to configure the VLAN blocking configuration shown in the Figure 5. The alternate
port is the neighbor with neighbor offset number 4. After manual preemption, VLANs 100 to 200 are blocked
at this port, and all the other VLANs are blocked at the primary edge port E1 (Gigabit Ethernet port 1/1).

Figure 31: Example of VLAN Blocking

Switch# configure terminal
Switch (conf)# interface gigabitethernet1/1
Switch (conf-if)# rep segment 1 edge primary
Switch (conf-if)# rep block port 4 vlan 100-200
Switch (conf-if)# end

Additional References for REP

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>REP commands</td>
<td></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the supported MIBs for this release.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at: <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 Resilient Ethernet Protocol

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 the 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>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilient Ethernet Protocol</td>
<td>Cisco IOS Release 15.2(6)E1</td>
<td>This feature was introduced. In Cisco IOS Release 15.2(6)E1, this feature is supported on Cisco Catalyst 2960-L Series Switches, Cisco Catalyst 2960-X Series Switches, and Cisco Digital Building.</td>
</tr>
</tbody>
</table>
CHAPTER 16

Configuring EtherChannels

• Finding Feature Information, on page 279
• Restrictions for EtherChannels, on page 279
• Information About EtherChannels, on page 280
• How to Configure EtherChannels, on page 289
• Monitoring EtherChannel, PAgP, and LACP Status, on page 301
• Configuration Examples for Configuring EtherChannels, on page 302
• Additional References for EtherChannels, on page 305
• Feature Information for EtherChannels, on page 306

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 (either Inter-Switch Link [ISL] or 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 32: Typical EtherChannel Configuration

The EtherChannel provides full-duplex bandwidth up to 8 Gb/s (Gigabit EtherChannel) or 40 Gb/s (10-Gigabit EtherChannel) between your switch and another switch or host. Note: Bandwidth up to 40 Gb/s (10-Gigabit EtherChannel) is supported with Cisco IOS Release 15.2(6)E and later releases.

Each EtherChannel can consist of up to eight compatibly configured Ethernet ports.

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 33: 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 6. 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 286
- Default EtherChannel Configuration
- Layer 2 EtherChannel Configuration Guidelines, on page 287
- 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 35: 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 289
- EtherChannel Configuration Guidelines, on page 286
- Default EtherChannel Configuration
- Layer 2 EtherChannel Configuration Guidelines, on page 287
- 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 289
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 switched 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.

Related Topics

- Related Topics
- Configuring the PAgP Learn Method and Priority, on page 291
- EtherChannel Configuration Guidelines, on page 286
- Default EtherChannel Configuration
- Monitoring EtherChannel, PAgP, and LACP Status, on page 301
- Layer 2 EtherChannel Configuration Guidelines, on page 287

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 CSCtn96950, 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>
<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**

Configure Layer 2 EtherChannels, on page 289
EtherChannel Configuration Guidelines, on page 286
Default EtherChannel Configuration
Layer 2 EtherChannel Configuration Guidelines, on page 287
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.

Default EtherChannel Configuration

The default EtherChannel configuration is described in this table.

Table 37: 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>
</tbody>
</table>
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 289
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, on page 289
  EtherChannel Overview
  EtherChannel Modes
  EtherChannel on Switches
  EtherChannel Link Failover
  LACP Modes, on page 284
  PAgP Modes, on page 282
  Silent Mode, on page 282
  Creating Port-Channel Logical Interfaces
  Channel Groups and Port-Channel Interfaces, on page 280
  Configuring the Physical Interfaces
  Configuring EtherChannel Load-Balancing
  Load-Balancing and Forwarding Methods
  MAC Address Forwarding
  IP Address Forwarding
  Load-Balancing Advantages
  Configuring the PAgP Learn Method and Priority, on page 291
  PAgP Learn Method and Priority, on page 283
  Configuring the LACP System Priority, on page 293
  Configuring the LACP Port Priority, on page 294
Load-Balancing and Forwarding Methods
MAC Address Forwarding
IP Address Forwarding
Load-Balancing Advantages
Configuring the PAgP Learn Method and Priority, on page 291
PAgP Learn Method and Priority, on page 283
Configuring the LACP System Priority, on page 293
Configuring the LACP Port Priority, on page 294

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>
<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 298
- Configuring Auto LAG: Examples, on page 303
- Configuring Auto-LAG on a Port Interface, on page 299
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 298
- Configuring Auto LAG: Examples, on page 303
- Configuring Auto-LAG on a Port Interface, on page 299
- Configuring Persistence with Auto-LAG, on page 300
- Auto-LAG, on page 288

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`
<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 a physical port, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Valid interfaces are physical ports.</td>
</tr>
<tr>
<td>Switch(config)# interface</td>
<td>For a PAgP EtherChannel, you can configure up to eight</td>
</tr>
<tr>
<td>gigabitethernet0/1</td>
<td>ports of the same type and speed for the same group.</td>
</tr>
<tr>
<td></td>
<td>For a LACP EtherChannel, you can configure up to 16</td>
</tr>
<tr>
<td></td>
<td>Ethernet ports of the same type. Up to eight ports can be active, and</td>
</tr>
<tr>
<td></td>
<td>up to eight ports can be in standby mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>switchport mode {access</td>
<td>Assigns all ports as static-access ports in the same VLAN, or configure</td>
</tr>
<tr>
<td></td>
<td>trunk}</td>
</tr>
<tr>
<td>Example:</td>
<td>If you configure the port as a static-access port, assign it to only</td>
</tr>
<tr>
<td>Switch(config-if)#</td>
<td>one VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td>switchport mode access</td>
<td></td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(Optional) If you configure the port as a static-access port, assign it</td>
</tr>
<tr>
<td>Example:</td>
<td>to only one VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td>Switch(config-if)#</td>
<td></td>
</tr>
<tr>
<td>switchport access vlan</td>
<td></td>
</tr>
<tr>
<td>vlan-id</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>channel-group channel-group-number mode {auto</td>
<td>Assigns the port to a channel group, and specifies the PAgP</td>
</tr>
<tr>
<td>[non-silent]</td>
<td>desirable [non-silent]</td>
</tr>
<tr>
<td>[on]</td>
<td>active</td>
</tr>
<tr>
<td>passive}</td>
<td>For mode, select one of these keywords:</td>
</tr>
<tr>
<td>Example:</td>
<td>• <strong>auto</strong>—Enables PAgP only if a PAgP device is detected. It places</td>
</tr>
<tr>
<td>Switch(config-if)#</td>
<td>the port into a passive negotiating state, in which the port responds</td>
</tr>
<tr>
<td>channel-group 5 mode auto</td>
<td>to PAgP packets it receives but does not start PAgP packet negotiation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>desirable</strong>—Unconditionally enables PAgP. It places the port into</td>
</tr>
<tr>
<td></td>
<td>an active negotiating state, in which the port starts negotiations with</td>
</tr>
<tr>
<td></td>
<td>other ports by sending PAgP packets.</td>
</tr>
<tr>
<td></td>
<td>• <strong>on</strong>—Forces the port to channel without PAgP or LACP. In the on</td>
</tr>
<tr>
<td></td>
<td>mode, an EtherChannel exists only when a port group in the on mode is</td>
</tr>
<tr>
<td></td>
<td>connected to another port group in the on mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>non-silent</strong> — (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 <strong>auto</strong> or <strong>desirable</strong> mode. If you do not specify <strong>non-silent</strong>, 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.</td>
</tr>
<tr>
<td>• <strong>active</strong> — 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>
</tr>
<tr>
<td>• <strong>passive</strong> — 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>
</tr>
</tbody>
</table>

### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config-if)# end
```

### Related Topics

- EtherChannel Overview
- EtherChannel Modes
- EtherChannel on Switches
- EtherChannel Link Failover
- LACP Modes, on page 284
- PAgP Modes, on page 282
- Silent Mode, on page 282
- EtherChannel Configuration Guidelines, on page 286
- Default EtherChannel Configuration
- Layer 2 EtherChannel Configuration Guidelines, on page 287

## 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
### 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>
</tbody>
</table>

| **Step 2** interface interface-id           | Specifies the port for transmission, and enters interface configuration mode. |
| Example:                                    |                                                                         |
| Switch(config)# interface gigabitethernet 0/2|                                                                         |

| **Step 3** pagp learn-method physical-port  | Selects the PAgP learning method.                                        |
| Example:                                    |                                                                         |
| Switch(config-if)# pagp learn-method physical-port |                                                |

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.

| **Step 4** pagp port-priority priority      | Assigns a priority so that the selected port is chosen for packet transmission. |
| Example:                                    |                                                                         |
| Switch(config-if)# pagp port-priority 200   |                                                                         |

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.

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

**Related Topics**

- PAgP Learn Method and Priority, on page 283
- EtherChannel Configuration Guidelines, on page 286
- Default EtherChannel Configuration
- Monitoring EtherChannel, PAgP, and LACP Status, on page 301
- Layer 2 EtherChannel Configuration Guidelines, on page 287
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>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 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).

### 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.

Follow these steps to configure the LACP port priority. This procedure is optional.

### SUMMARY STEPS

1. `enable`

---

### Command or Action | Purpose
---|---
**Example:**
Switch> `enable`
• Enter your password if prompted.

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

**Step 3**
lACP system-priority `priority`
**Example:**
Switch(config)# `lacp system-priority 32000`
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**
end
**Example:**
Switch(config)# `end`
Returns to privileged EXEC mode.

### Related Topics
- EtherChannel Configuration Guidelines, on page 286
- Default EtherChannel Configuration
- Layer 2 EtherChannel Configuration Guidelines, on page 287
- Monitoring EtherChannel, PAgP, and LACP Status, on page 301
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>
<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# 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><strong>Example:</strong> Switch(config)# interface gigabitethernet 0/2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> lACP port-priority priority</td>
<td>Configures the LACP port priority.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# lACP port-priority 32000</td>
<td>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.</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>

**Related Topics**
- EtherChannel Configuration Guidelines, on page 286
- Default EtherChannel Configuration
- Layer 2 EtherChannel Configuration Guidelines, on page 287
- Monitoring EtherChannel, PAgP, and LACP Status, on page 301
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><em>Enter your password if prompted.</em></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** interface port-channel *channel-number* | Enters interface configuration mode for a port-channel. |
| Example:                                          | For *channel-number*, the range is 1 to 6. |
| Switch(config)# interface port-channel 2         | |

| **Step 4** port-channel min-links *min-links-number* | 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. |
| Example:                                          | For *min-links-number*, the range is 2 to 8. |
| Switch(config-if)# port-channel min-links 3       | |

| **Step 5** end | Returns to privileged EXEC mode. |
| Example:       | |
| Switch(config)# end | |
Related Topics

Configuring LACP Port Channel Min-Links: Examples, on page 304

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>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> interface { fastethernet</td>
<td>gigabitethernet</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# interface gigabitEthernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> lacp rate { normal</td>
<td>fast }</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# lacp rate fast</td>
<td>• To reset the timeout rate to its default, use the <code>no lacp rate</code> command.</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>
</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></td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch&gt; enable</code>&lt;br&gt;Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</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 3</strong></td>
<td><code>[no] port-channel auto</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;<code>Switch(config)# port-channel auto</code>&lt;br&gt;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.&lt;br&gt;<strong>Note</strong> By default, the auto-LAG feature is enabled on the port.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Related Topics**

Example: Configuring LACP Fast Rate Timer, on page 304
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><strong>Enables privileged EXEC mode.</strong></td>
</tr>
<tr>
<td>enable</td>
<td><strong>Enables privileged EXEC mode.</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enter your password if prompted.</strong></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td><strong>Enter your password if prompted.</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**Specifies the port interface to be enabled for auto-LAG, and enters <strong>interface configuration mode.</strong></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>**Specifies the port interface to be enabled for auto-LAG, and enters <strong>interface configuration mode.</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>**Specifies the port interface to be enabled for auto-LAG, and enters <strong>interface configuration mode.</strong></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td>**Specifies the port interface to be enabled for auto-LAG, and enters <strong>interface configuration mode.</strong></td>
</tr>
</tbody>
</table>

**Related Topics**

- Auto-LAG, on page 288
- Auto-LAG Configuration Guidelines, on page 289
- Configuring Auto LAG: Examples, on page 303
- Configuring Auto-LAG on a Port Interface, on page 299
- Configuring Persistence with Auto-LAG, on page 300
### Purpose

**Command or Action**

**Step 4**

```
(no) channel-group auto
```

**Example:**

```
Switch(config-if)# channel-group auto
```

- **Purpose:** (Optional) Enables auto-LAG feature on individual port interface. Use the no form of this command to disable the auto-LAG feature on individual port interface.

- **Note:** By default, the auto-LAG feature is enabled on the port.

**Step 5**

```
end
```

**Example:**

```
Switch(config-if)# end
```

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

**Step 6**

```
show etherchannel auto
```

**Example:**

```
Switch# show etherchannel auto
```

- **Purpose:** Displays that EtherChannel is created automatically.

---

### What to do next

Related Topics

- Configuring Auto-LAG Globally, on page 298
- Auto-LAG, on page 288
- Auto-LAG Configuration Guidelines, on page 289
- Configuring Persistence with Auto-LAG, on page 300
- Configuring Auto LAG: Examples, on page 303

---

### 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><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| **Example:**
```
Switch> enable
```
| | - Enter your password if prompted. |
| **Step 2** `port-channel channel-number persistent` | Converts the auto created EtherChannel into a manual one and allows you to add configuration on the EtherChannel. |
| **Example:** | |

---
Monitoring EtherChannel, PAgP, and LACP Status

You can display EtherChannel, PAgP, and LACP status using the commands listed in this table.

Table 39: Commands for Monitoring EtherChannel, PAgP, and LACP Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear lacp</code> (channel-group-number) counters</td>
<td>Clears LACP channel-group information and traffic counters.</td>
</tr>
<tr>
<td><code>clear pagp</code> (channel-group-number) counters</td>
<td>Clears PAgP channel-group information and traffic counters.</td>
</tr>
<tr>
<td><code>show etherchannel</code> (channel-group-number) [detail</td>
<td>load-balance</td>
</tr>
<tr>
<td><code>show pagp</code> (channel-group-number) [counters</td>
<td>internal</td>
</tr>
<tr>
<td><code>show pagp</code> (channel-group-number) dual-active</td>
<td>Displays the dual-active detection status.</td>
</tr>
<tr>
<td><code>show lacp</code> (channel-group-number) [counters</td>
<td>internal</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your configuration entries.</td>
</tr>
<tr>
<td><code>show etherchannel load-balance</code></td>
<td>Displays the load balance or frame distribution scheme among ports in the port channel.</td>
</tr>
</tbody>
</table>
Related Topics

- Configuring the PAgP Learn Method and Priority, on page 291
- PAgP Learn Method and Priority, on page 283
- Configuring the LACP System Priority, on page 293
- Configuring the LACP Port Priority, on page 294

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 gigabitethernet0/1 -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 gigabitethernet0/1 -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`
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
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(SU) | LACP       | Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)                  |
```

Related Topics:
- Configuring Auto-LAG Globally, on page 298
- Auto-LAG, on page 288
- Auto-LAG Configuration Guidelines, on page 289
- Configuring Persistence with Auto-LAG, on page 300
- Configuring Auto-LAG on a Port Interface, on page 299
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# show etherchannel 25 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

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Po25(RM)</td>
<td>LACP</td>
<td>Gi1/3/1(D) Gi1/3/2(D) Gi2/2/25(D) Gi2/2/26(W)</td>
</tr>
</tbody>
</table>
```

Related Topics

- [Configuring the LACP Port Channel Min-Links Feature](#), on page 296

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
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
```
The following is sample output from the `show lACP counters` command:

```
switch# show lACP counters
LACPDUs Marker Marker Response LACPDUs
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 297

## 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></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 the 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

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

http://www.cisco.com/support

Feature Information for EtherChannels

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>
Configuring Link-State Tracking

- Finding Feature Information, on page 307
- Restrictions for Configuring Link-State Tracking, on page 307
- Understanding Link-State Tracking, on page 308
- How to Configure Link-State Tracking, on page 310
- Monitoring Link-State Tracking, on page 311
- Configuring Link-State Tracking: Example, on page 311
- Feature Information for Link-State Tracking, on page 311

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 Link-State Tracking

- You can configure only two link-state groups per switch.
- An interface cannot be a member of more than one link-state group.
- An interface that is defined as an upstream interface in a link-state group cannot also be defined as a downstream interface in the link-state group.
- Do not enable link-state tracking on individual interfaces that will part of a downstream EtherChannel interface.
- Add the upstream interfaces to the link state group before adding the downstream interfaces. Otherwise, the downstream interface is put in error-disabled state.
• When a downstream interface is configured as a SPAN destination port, it is placed in error-disabled state when all upstream interfaces in its group are down. When an upstream interface is configured as a SPAN destination port, it is considered as a link-down event on the interface.

Understanding Link-State Tracking

Link-state tracking, also known as trunk failover, binds the link state of multiple interfaces. Link-state tracking can be with server NIC adapter teaming to provide redundancy in the network. When the server NIC adapters are configured in a primary or secondary relationship, and the link is lost on the primary interface, network connectivity is transparently changed to the secondary interface.

Note

An interface can be an aggregation of ports (an EtherChannel) or a single physical port in either access or trunk mode.

The configuration in this figure ensures that the network traffic flow is balanced.

Figure 34: Typical Link-State Tracking Configuration

• For links to switches and other network devices
• Server 1 and server 2 use switch A for primary links and switch B for secondary links.
• Server 3 and server 4 use switch B for primary links and switch A for secondary links.

• Link-state group 1 on switch A
  • Switch A provides primary links to server 1 and server 2 through link-state group 1. Port 1 is connected to server 1, and port 2 is connected to server 2. Port 1 and port 2 are the downstream interfaces in link-state group 1.
  • Port 5 and port 6 are connected to distribution switch 1 through link-state group 1. Port 5 and port 6 are the upstream interfaces in link-state group 1.

• Link-state group 2 on switch A
  • Switch A provides secondary links to server 3 and server 4 through link-state group 2. Port 3 is connected to server 3, and port 4 is connected to server 4. Port 3 and port 4 are the downstream interfaces in link-state group 2.
  • Port 7 and port 8 are connected to distribution switch 2 through link-state group 2. Port 7 and port 8 are the upstream interfaces in link-state group 2.

• Link-state group 2 on switch B
  • Switch B provides primary links to server 3 and server 4 through link-state group 2. Port 3 is connected to server 3, and port 4 is connected to server 4. Port 3 and port 4 are the downstream interfaces in link-state group 2.
  • Port 5 and port 6 are connected to distribution switch 2 through link-state group 2. Port 5 and port 6 are the upstream interfaces in link-state group 2.

• Link-state group 1 on switch B
  • Switch B provides secondary links to server 1 and server 2 through link-state group 1. Port 1 is connected to server 1, and port 2 is connected to server 2. Port 1 and port 2 are the downstream interfaces in link-state group 1.
  • Port 7 and port 8 are connected to distribution switch 1 through link-state group 1. Port 7 and port 8 are the upstream interfaces in link-state group 1.

In a link-state group, the upstream ports can become unavailable or lose connectivity because the distribution switch or router fails, the cables are disconnected, or the link is lost. These are the interactions between the downstream and upstream interfaces when link-state tracking is enabled:

• If any of the upstream interfaces are in the link-up state, the downstream interfaces can change to or remain in the link-up state.

• If all of the upstream interfaces become unavailable, link-state tracking automatically puts the downstream interfaces in the error-disabled state. Connectivity to and from the servers is automatically changed from the primary server interface to the secondary server interface. For example, in the previous figure, if the upstream link for port 6 is lost, the link states of downstream ports 1 and 2 do not change. However, if the link for upstream port 5 is also lost, the link state of the downstream ports changes to the link-down state. Connectivity to server 1 and server 2 is then changed from link-state group 1 to link-state group 2. The downstream ports 3 and 4 do not change state because they are in link-group 2.
If the link-state group is configured, link-state tracking is disabled, and the upstream interfaces lose connectivity, the link states of the downstream interfaces remain unchanged. The server does not recognize that upstream connectivity has been lost and does not failover to the secondary interface.

You can recover a downstream interface link-down condition by removing the failed downstream port from the link-state group. To recover multiple downstream interfaces, disable the link-state group.

How to Configure Link-State Tracking

To enable link-state tracking, create a link-state group and specify the interfaces that are assigned to the group. This task is optional.

**SUMMARY STEPS**

1. configure terminal
2. link state track number
3. interface interface-id
4. link state group \[number\]{upstream | downstream}
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: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 link state track number</td>
<td>Creates a link-state group and enables link-state tracking. The group number can be 1 or 2; the default is 1.</td>
</tr>
<tr>
<td>Example: Switch(config)# link state track 2</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Specifies a physical interface or range of interfaces to configure, and enters interface configuration mode. Valid interfaces include switch ports in access or trunk mode (IEEE 802.1q) or routed ports.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet0/1</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Do not enable link-state tracking on individual interfaces that will be part of an Etherchannel interface.</td>
</tr>
<tr>
<td>Step 4 link state group [number]{upstream</td>
<td>downstream}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring Link-State Tracking

You can display link-state tracking status using the command in this table.

**Table 40: Commands for Monitoring Link-State Tracking Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show link state group [number] [detail]</code></td>
<td>Displays the link-state group information.</td>
</tr>
</tbody>
</table>

### Configuring Link-State Tracking: Example

This example shows how to create the link-state group 1 and configure the interfaces in the link-state group.

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config-if)# interface range gigabitethernet0/21-22
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface gigabitethernet0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface gigabitethernet0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

### Feature Information for Link-State Tracking

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS 15.2(6)E1</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

---

*Source: Layer 2, Monitoring Link-State Tracking, Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)*
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 has 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 disconnected 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 detect 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 316
- Enabling UDLD on an Interface, on page 318

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 heart beat whose presence guarantees the health of the link. Conversely, the loss of the heart beat 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 316
- Enabling UDLD on an Interface, on page 318

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 316
- Enabling UDLD on an Interface, on page 318

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 316
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 316
- Enabling UDLD on an Interface, on page 318

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 316
- Enabling UDLD on an Interface, on page 318

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><strong>Step 1</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 2</strong></td>
<td>Specifies the UDLD mode of operation:</td>
</tr>
<tr>
<td>`udld {aggressive</td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# udld enable message time 10</code></td>
<td></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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Monitoring and Maintaing UDLD
- Aggressive Mode, on page 314
- Normal Mode, on page 314
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> 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 enabled for UDLD, and enters interface configuration mode.</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> udld port [aggressive]</td>
<td>UDLD is disabled by default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# udld port aggressive</td>
<td>• udld port—Enables UDLD in normal mode on the specified port.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• udld port aggressive—(Optional) Enables UDLD in aggressive mode on the specified port.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use the no udld port interface configuration command to disable UDLD on a specified fiber-optic port.</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-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
Related Topics
- Monitoring and Maintaining UDLD
- Aggressive Mode, on page 314
- Normal Mode, on page 314
- Methods to Detect Unidirectional Links, on page 315
- Event-Driven Detection and Echoing, on page 315
- UDLD Reset Options, on page 316
- Default UDLD Configuration, on page 316

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>For complete syntax and usage information for the commands used in this chapter.</td>
<td></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 the 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 for UDLD

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 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 323
- Configuring the Cisco Discovery Protocol, on page 335
- Configuring Simple Network Management Protocol, on page 347
- Configuring SPAN, on page 371
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)

---

**Note**

Support for Cisco Configuration Engine will be deprecated in future releases. Use the configuration described in Cisco Plug and Play Feature Guide.

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 35: 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 42: 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</td>
</tr>
<tr>
<td></td>
<td>• IP routing (if used as default gateway)</td>
</tr>
<tr>
<td>Device</td>
<td>Required Configuration</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------</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>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>

2 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

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><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> cns event {hostname</td>
<td>ip-address} [port-number] [keepalive seconds retry-count] [failover-time seconds] [reconnect-time time]</td>
</tr>
<tr>
<td><strong>Example:</strong> 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>
<tr>
<td></td>
<td>• (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.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For reconnect-time time, enter the maximum time interval that the switch waits before trying to reconnect to the event gateway.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Enter backup to show that this is the backup gateway. (If omitted, this is the primary gateway.)</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)# end</td>
<td>Note: Though visible in the command-line help string, the encrypt and the clock-timeout time keywords are not supported.</td>
</tr>
</tbody>
</table>
### Purpose

#### Step 5

**Command or Action**: `show running-config`  
**Purpose**: Verifies your entries.

**Example**:  
```bash  
Switch# show running-config  
```

#### Step 6

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

**Example**:  
```bash  
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>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
| `Example:` | • Enter your password if prompted.  

```bash  
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch&gt; enable</td>
<td>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.</td>
</tr>
</tbody>
</table>
| **Step 2** show cns config connections  
  Example:  
  Switch# show cns config connections | 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 3** Make sure that the CNS event agent is properly connected to the event gateway. | Displays the event connection information for your switch. |
| **Step 4** show cns event connections  
  Example:  
  Switch# show cns event connections | Enters global configuration mode. |
| **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. | Specifies the IP address and port number that you recorded in Step 5 in this command.  
  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. |
| **Step 6** configure terminal  
  Example:  
  Switch# configure terminal | Specifies the IP address and port number that you recorded in Step 5 in this command.  
  This command reestablishes the connection between the switch and the event gateway. |
| **Step 7** no cns event ip-address port-number  
  Example:  
  Switch(config)# no cns event 172.28.129.22 2012 | Returns to privileged EXEC mode. |
| **Step 8** cns event ip-address port-number  
  Example:  
  Switch(config)# cns event 172.28.129.22 2012 | |
| **Step 9** end  
  Example:  
  Switch(config)# end | |

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
## Monitoring CNS Configurations

### Table 43: CNS show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cns config connections</code></td>
<td>Displays the status of the CNS Cisco IOS CNS agent connections.</td>
</tr>
<tr>
<td><code>show cns config outstanding</code></td>
<td>Displays information about incremental (partial) CNS configurations that have started but are not yet completed.</td>
</tr>
<tr>
<td><code>show cns config stats</code></td>
<td>Displays statistics about the Cisco IOS CNS agent.</td>
</tr>
<tr>
<td><code>show cns event connections</code></td>
<td>Displays the status of the CNS event agent connections.</td>
</tr>
<tr>
<td><code>show cns event gateway</code></td>
<td>Displays the event gateway information for your switch.</td>
</tr>
<tr>
<td><code>show cns event stats</code></td>
<td>Displays statistics about the CNS event agent.</td>
</tr>
</tbody>
</table>

---

**Step 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`.

**Step 11**
- `show running-config`
  - **Example:**
    ```
    Switch# show running-config
    ```

**Step 12**
- `copy running-config startup-config`
  - **Example:**
    ```
    Switch# copy running-config startup-config
    ```

(Optional) Saves your entries in the configuration file.
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cns event subject</td>
<td>Displays a list of event agent subjects that are subscribed to by applications.</td>
</tr>
</tbody>
</table>

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Engine Setup</td>
<td><em>Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux</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 the 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 the Configuration Engine

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring the Cisco Discovery Protocol

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that runs on Cisco devices and enables networking applications to learn about directly connected devices nearby. This protocol facilitates the management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about each other.

This module describes Cisco Discovery Protocol Version 2 and how it functions with SNMP.

• Finding Feature Information, on page 335
• Information About CDP, on page 335
• How to Configure CDP, on page 336
• Monitoring and Maintaining Cisco Discovery Protocol, on page 344
• Additional References, on page 345
• Feature History and Information for Cisco Discovery Protocol, on page 346

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

Cisco Discovery Protocol Overview

Cisco Discovery Protocol 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 Cisco Discovery Protocol, network management applications can learn the device type and the SNMP agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.
Cisco Discovery Protocol runs on all media that support Subnetwork Access Protocol (SNAP). Because Cisco Discovery Protocol runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each Cisco Discovery Protocol-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 Cisco Discovery Protocol information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

On the switch, Cisco Discovery Protocol enables Network Assistant to display a graphical view of the network. The switch uses Cisco Discovery Protocol 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.

- Cisco Discovery Protocol identifies connected endpoints that communicate directly with the switch.
- To prevent duplicate reports of neighboring devices, only one wired switch reports the location information.
- The wired switch and the endpoints both send and receive location information.

**Related Topics**
- [Configuring Cisco Discovery Protocol Characteristics](#), on page 336
- [Monitoring and Maintaining Cisco Discovery Protocol](#), on page 344

## Default Cisco Discovery Protocol Configuration

This table shows the default Cisco Discovery Protocol configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Discovery Protocol global state</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco Discovery Protocol interface state</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco Discovery Protocol timer (packet update frequency)</td>
<td>60 seconds</td>
</tr>
<tr>
<td>Cisco Discovery Protocol holdtime (before discarding)</td>
<td>180 seconds</td>
</tr>
<tr>
<td>Cisco Discovery Protocol Version-2 advertisements</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Related Topics**
- [Enabling Cisco Discovery Protocol](#), on page 340
- [Disabling Cisco Discovery Protocol](#), on page 338
- [Enabling Cisco Discovery Protocol on an Interface](#), on page 343
- [Disabling Cisco Discovery Protocol on an Interface](#), on page 341

## How to Configure CDP

### Configuring Cisco Discovery Protocol Characteristics

You can configure these Cisco Discovery Protocol characteristics:
• Frequency of Cisco Discovery Protocol 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 Cisco Discovery Protocol 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>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><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>cdp timer seconds</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Sets the transmission frequency of Cisco Discovery Protocol updates in seconds.</td>
</tr>
<tr>
<td></td>
<td>The range is 5 to 254; the default is 60 seconds.</td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# cdp timer 20</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>cdp holdtime seconds</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Specifies the amount of time a receiving device should hold the information sent by your device before discarding it.</td>
</tr>
<tr>
<td></td>
<td>The range is 10 to 255 seconds; the default is 180 seconds.</td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# cdp holdtime 60</code></td>
</tr>
</tbody>
</table>
### Disabling Cisco Discovery Protocol

Cisco Discovery Protocol is enabled by default.

#### 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.

Follow these steps to disable the Cisco Discovery Protocol 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

### 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:  
   Switch> enable |  
| 2    | configure terminal | Enters global configuration mode.  
   Example:  
   Switch# configure terminal |  
| 3    | no cdp run | Disables Cisco Discovery Protocol.  
   Example:  
   Switch(config)# no cdp run |  
| 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 |  

### What to do next

You must reenable Cisco Discovery Protocol to use it.

### Related Topics

- [Enabling Cisco Discovery Protocol](#), on page 340
- Default Cisco Discovery Protocol Configuration, on page 336
Enabling Cisco Discovery Protocol

Cisco Discovery Protocol is enabled by default.

**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.

Follow these steps to enable Cisco Discovery Protocol when it has been disabled.

**Before you begin**

Cisco Discovery Protocol 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>
<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: <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: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables Cisco Discovery Protocol if it has been disabled.</td>
</tr>
<tr>
<td><code>cdp run</code></td>
<td></td>
</tr>
<tr>
<td>Example: <code>Switch(config)# cdp run</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)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</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 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></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

Use the `show run all` command to show that Cisco Discovery Protocol has been enabled. If you enter only `show run`, the enabling of Cisco Discovery Protocol may not be displayed.

### Related Topics

- Default Cisco Discovery Protocol Configuration, on page 336
- Disabling Cisco Discovery Protocol, on page 338

### 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>
</table>
| **Step 1** | Enables privileged EXEC mode.  
  Example:  
  Switch> enable |
| **Step 2** | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** | Specifies the interface on which you are disabling Cisco Discovery Protocol, and enters interface configuration mode.  
  Example:  
  Switch(config)# interface gigabitethernet 0/1 |
| **Step 4** | Disables Cisco Discovery Protocol on the interface specified in Step 3.  
  Example:  
  Switch(config-if)# no cdp enable |
| **Step 5** | Returns to privileged EXEC mode.  
  Example:  
  Switch(config)# end |
| **Step 6** | Verifies your entries.  
  Example:  
  Switch# show running-config |
| **Step 7** | (Optional) Saves your entries in the configuration file.  
  Example:  
  Switch# copy running-config startup-config |

**Related Topics**

- Enabling Cisco Discovery Protocol on an Interface, on page 343
- Default Cisco Discovery Protocol Configuration, on page 336
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>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></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>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet0/1</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cdp enable</code></td>
<td>Enables Cisco Discovery Protocol on a disabled interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch(config-if)# cdp enable
```

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

**Example:**

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

**Step 6**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>

**Example:**

```
Switch# show running-config
```

**Step 7**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Example:**

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

---

### Related Topics

- Default Cisco Discovery Protocol Configuration, on page 336
- Disabling Cisco Discovery Protocol on an Interface, on page 341

---

### Monitoring and Maintaining Cisco Discovery Protocol

---

### Table 44: Commands for Displaying Cisco Discovery Protocol 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 Cisco Discovery Protocol 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>
</tbody>
</table>
Command | Description
--- | ---
show cdp entry entry-name [version] [protocol] | Displays information about a specific neighbor. You can enter an asterisk (*) to display all Cisco Discovery Protocol 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.
show cdp interface [interface-id] | Displays information about interfaces where Cisco Discovery Protocol is enabled. You can limit the display to the interface about which you want information.
show cdp neighbors [interface-id] [detail] | 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.
show cdp traffic | Displays Cisco Discovery Protocol counters, including the number of packets sent and received and checksum errors.

Related Topics
- Configuring Cisco Discovery Protocol Characteristics, on page 336
- Cisco Discovery Protocol Overview, on page 335

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></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 History and Information for Cisco Discovery Protocol

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

3 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.

4 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.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.
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.

SNMP MIB Variables Access

An example of an NMS is the Cisco Prime Infrastructure network management software. Cisco Prime Infrastructure 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.

**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(^5)</td>
<td>1–4999</td>
</tr>
<tr>
<td>EtherChannel</td>
<td>5001–5048</td>
</tr>
<tr>
<td>Tunnel</td>
<td>5078–5142</td>
</tr>
<tr>
<td>Physical (such as Gigabit Ethernet or SFP(^6)-module interfaces) based on type and port numbers</td>
<td>10000–14500</td>
</tr>
<tr>
<td>Null</td>
<td>14501</td>
</tr>
<tr>
<td>Loopback and Tunnel</td>
<td>24567+</td>
</tr>
</tbody>
</table>

\(^5\) 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>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------</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.
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>Step</th>
<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** | no snmp-server  
*Example:*  
Switch(config)# no snmp-server | Disables the SNMP agent operation. |
| **Step 4** | end  
*Example:* | Returns to privileged EXEC mode. |
### 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>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>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></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>
<td>Configures the community string. <strong>Note</strong> 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><strong>Example:</strong> Switch(config)# snmp-server community comaccess ro 4</td>
<td>• For string, 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>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Optional) For view, specify the view record accessible to the community.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Optional) Specify either read-only (ro) if you want authorized management stations to retrieve MIB objects, or specify read-write (rw) 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>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Optional) For access-list-number, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]</td>
<td>(Optional) If you specified an IP standard access list number in Step 3, then create the list, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# access-list 4 deny any</td>
<td>• For access-list-number, enter the access list number specified in Step 3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For source, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Step 5**

**Command or Action:** `end`  
**Example:**

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

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

**Step 6**

**Command or Action:** `show running-config`  
**Example:**

```
Switch# show running-config
```

**Purpose:** Verifies your entries.

**Step 7**

**Command or Action:** `copy running-config startup-config`  
**Example:**

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

**Purpose:** (Optional) Saves your entries in the configuration file.

### 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 communitystring globalconfiguration` 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]} engineid-string`
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]}`
### 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><em>enable</em></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><em>Switch&gt; enable</em></td>
<td></td>
</tr>
</tbody>
</table>

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

| **Step 3**         |         |
| *snmp-server engineID [local engineid-string | remote ip-address [udp-port port-number] engineid-string]* | 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 Example configures an engine ID of 123400000000000000000000. |
| *Switch(config)# snmp-server engineID local 1234* | • 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. |

| **Step 4**         |         |
| *snmp-server group group-name {v1 | v2c | v3 {auth | noauth | priv}} [read readview] [write writeview] [notify notifyview] [access access-list]* | Configures a new SNMP group on the remote device. |
| **Example:**       | For *group-name*, specify the name of the group. Specify one of the following security models: |
| *Switch(config)# snmp-server group public v2c access lmnop* | • *v1* is the least secure of the possible security models. |
|                     | • *v2c* is the second least secure model. It allows transmission of informs and integers twice the normal width. |
|                     | • *v3*, the most secure, requires you to select one of the following authentication levels: |
|                     | *auth*—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication. |
**Purpose**

- **noauth**—Enables the noAuthNoPriv security level. This is the default if no keyword is specified.

- **priv**—Enables Data Encryption Standard (DES) packet encryption (also called privacy).

(Optional) Enter **read readview** 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.

(Optional) Enter **write writeview** 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.

(Optional) Enter **notify notifyview** with a string (not to exceed 64 characters) that is the name of the view in which you specify a notify, inform, or trap.

(Optional) Enter **access access-list** with a string (not to exceed 64 characters) that is the name of the access list.

---

**Step 5**

```plaintext
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]
```

 Adds a new user for an SNMP group.

The **username** is the name of the user on the host that connects to the agent.

The **group-name** is the name of the group to which the user is associated.

Enter **remote** to specify a remote SNMP entity to which the user belongs and the hostname or IP address of that 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:

- **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.
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.

Note
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 48: 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>Notification Type Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</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>hsrp</td>
<td>Generates a trap for Hot Standby Router Protocol (HSRP) changes.</td>
</tr>
<tr>
<td>ipmulticast</td>
<td>Generates a trap for IP multicast routing changes.</td>
</tr>
<tr>
<td>ipsla</td>
<td>Generates a trap for the SNMP IP Service Level Agreements (SLAs).</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>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` |
| snmp                      | Generates a trap for SNMP-type notifications for authentication, cold start, warm start, link up or link down. |
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).

Generates SNMP STP Extended MIB traps.

Generates SNMP syslog traps.

Generates a trap for TCP connections. This trap is enabled by default.

Generates a trap for SNMP VLAN membership changes.

Generates SNMP VLAN created traps.

Generates SNMP VLAN deleted traps.

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]
6. snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 {auth | noauth | priv}}] [community-string [notification-type]]
7. snmp-server enable traps notification-types
8. snmp-server trap-source interface-id
9. snmp-server queue-length length
10. snmp-server trap-timeout seconds
11. end
12. show running-config
13. 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>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>snmp-server engineID remote ip-address engineid-string</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**snmp-server user username group-name { remote host [ udp-port port ] } [ v1 [ access access-list ]</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**snmp-server group group-name { v1</td>
</tr>
</tbody>
</table>
| **Step 6** | **snmp-server host host-addr [ informs | traps ] [ version { 1 | 2c | 3 { auth | noauth | priv } } ] community-string [ notification-type ]**<br>**Example:**<br>Switch(config)# snmp-server host 203.0.113.1 comaccess snmp | Specifies the recipient of an SNMP trap operation. For `host-addr`, specify the name or Internet address of the host (the targeted recipient).<br>(Optional) Specify `traps` (the default) to send SNMP traps to the host.<br>(Optional) Specify `informs` to send SNMP informs to the host.<br>(Optional) Specify the SNMP version (`1`, `2c`, or `3`). SNMPv1 does not support informs.<br>(Optional) For Version 3, select authentication level `auth`, `noauth`, or `priv`.<br>**Note** The `priv` keyword is available only when the cryptographic software image is installed.<br>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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>(Optional) For notification-type, use the keywords listed in the table above. If no type is specified, all notifications are sent.</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Step 7**

`snmp-server enable traps notification-types`<br>
**Example:**  
`Switch(config)# snmp-server enable traps snmp`<br>

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:  

a. `snmp-server enable traps port-security`  
b. `snmp-server enable traps port-security trap-rate rate`  

**Step 8**

`snmp-server trap-source interface-id`<br>
**Example:**  
`Switch(config)# snmp-server trap-source gigabitethernet 0/1`<br>

(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`<br>
**Example:**  
`Switch(config)# snmp-server queue-length 20`<br>

(Optional) Establishes the message queue length for each trap host. The range is 1 to 5000; the default is 10.  

**Step 10**

`snmp-server trap-timeout seconds`<br>
**Example:**  
`Switch(config)# snmp-server trap-timeout 60`<br>

(Optional) Defines how often to resend trap messages. The range is 1 to 1000; the default is 30 seconds.  

**Step 11**

`end`<br>
**Example:**  
`Switch(config)# end`<br>

Returns to privileged EXEC mode.  

**Step 12**

`show running-config`<br>
**Example:**  
`Switch# show running-config`<br>

Verifies your entries.
Step 13  |  copy running-config startup-config  
Example:  |  Switch# copy running-config startup-config  

(Optional) Saves your entries in the configuration file.

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.

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>
<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>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>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### 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>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**  
**snmp-server tftp-server-list** `access-list-number`  
**Example:**  
Switch(config)# snmp-server tftp-server-list 44 | Limits the TFTP servers used for configuration file copies through SNMP to the servers in the access list.  
For `access-list-number`, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. |
| **Step 4**  
**access-list** `access-list-number` {deny | permit} `source` [source-wildcard]  
**Example:**  
Switch(config)# access-list 44 permit 10.1.1.2 | Creates a standard access 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 TFTP servers that can access the switch.  
(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.  
The access list is always terminated by an implicit deny statement for everything. |
| **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. |
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 49: 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></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 group</td>
<td>Displays information on each SNMP group on the network.</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>
<tr>
<td>show snmp user</td>
<td>Displays information on each SNMP user name in the SNMP users table.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You must use this command to display SNMPv3 configuration information for `auth</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 user authuser authgroup 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></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L 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>
</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 Simple Network Management Protocol

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

• Finding Feature Information, on page 371
• Restrictions for SPAN, on page 371
• Information About SPAN, on page 372
• How to Configure SPAN, on page 373
• Monitoring SPAN Operations, on page 377
• SPAN Configuration Examples, on page 377
• Additional References, on page 378
• Feature History and Information for SPAN, on page 379

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.

• You cannot have two SPAN sessions using the same source 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 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 up to four local SPAN sessions.

• 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>
</tbody>
</table>
### Configuration Guidelines

#### SPAN Configuration Guidelines

- To remove a source or destination port from the SPAN session, use the `no monitor session session_number source interface interface-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>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:** | Enters global configuration mode. |
### 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

**no monitor session session_number**

**Example:**

Switch(config)# no monitor session 1

**Switch\# configure terminal**

Removing 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

**Switch(config)# configure terminal**

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

**Switch(config)# configure terminal**

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.
### 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`
4. `monitor session session_number source {interface interface-id} [, | -] [both | rx | tx]`
5. `monitor session session_number destination {interface interface-id [encapsulation replicate ingress {vlan vlan-id} | ingress {vlan vlan-id}]}`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Note**

You can use `monitor session session_number destination` command multiple times to configure multiple destination ports.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For <code>interface-id</code>, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) [,</td>
<td>-] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</td>
</tr>
</tbody>
</table>
## 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** no monitor session *session_number* | Removes existing SPAN configuration for the specified session. The range is 1 to 4.  
  Example:  
  Switch(config)# no monitor session 1 |
| **Step 4** monitor session *session_number* source {interface *interface-id*} [rx | tx] | Specifies the SPAN session and the source port (monitored port).  
  Example:  
  Switch(config)# monitor session 2 source gigabitethernet0/1 rx |
| **Step 5** monitor session *session_number* destination {interface *interface-id*} [encapsulation replicate ingress {vlan *vlan-id*} | ingress {vlan *vlan-id*}] | Specifies the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation.  
  Example:  
  Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress vlan 6 |
| **Step 6** end | Returns to privileged EXEC mode.  
  Example:  
  Switch(config)# end |
Purpose
Command or Action

Switch(config)# end

Step 7 show running-config
Example:
Switch# show running-config

Step 8 copy running-config startup-config
Example:
Switch# copy running-config startup-config

Verifies your entries.

(Optional) Saves your entries in the configuration file.

Monitoring SPAN Operations

The following table describes the command used to display SPAN operations configuration and results to monitor operations:

Table 51: 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 all keyword to show configuration for all SPAN sessions, the local keyword to show configurations for local sessions only, and the range 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

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></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 the 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 SPAN

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)ECisco IOS 15.2(5)E</td>
<td>Switch Port Analyzer (SPAN): Allows monitoring of switch traffic on a port or VLAN using a sniffer/analyzer 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 15.2(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 15.2(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>
<tr>
<td>Cisco IOS Release 15.2(6)E2</td>
<td>Support for 4 SPAN sessions was introduced.</td>
</tr>
</tbody>
</table>
PART VI

QoS

• Configuring QoS, on page 383
• Configuring AutoQoS, on page 439
CHAPTER 23

Configuring QoS

- Finding Feature Information, on page 383
- Prerequisites for QoS, on page 383
- Restrictions for QoS, on page 384
- Information About QoS, on page 385
- How to Configure QoS, on page 399
- Monitoring Standard QoS, on page 431
- Configuration Examples for QoS, on page 432
- Where to Go Next, on page 437
- Feature History and Information for QoS, on page 437

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.

QoS ACL Guidelines

Follow these guidelines when configuring QoS with access control lists (ACLs):
• It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are sent as best-effort. IP fragments are denoted by fields in the IP header.

• Only one ACL per class map and only one **match** class-map configuration command per class map are supported. The ACL can have multiple ACEs, which match fields against the contents of the packet.

### Policing Guidelines

• Only one policer is applied to a packet on an ingress port. Only the average rate and committed burst parameters are configurable.

• On a port configured for QoS, all traffic received through the port is classified, policed, and marked according to the policy map attached to the port. On a trunk port configured for QoS, traffic in all VLANs received through the port is classified, policed, and marked according to the policy map attached to the port.

• If you have EtherChannel ports configured on your switch, you must configure QoS classification, policing, mapping, and queueing on the individual physical ports that comprise the EtherChannel. You must decide whether the QoS configuration should match on all ports in the EtherChannel.

• If you need to modify a policy map of an existing QoS policy, first remove the policy map from all interfaces, and then modify or copy the policy map. After you finish the modification, apply the modified policy map to the interfaces. If you do not first remove the policy map from all interfaces, high CPU usage can occur, which, in turn, can cause the console to pause for a very long time.

### General QoS Guidelines

These are the general QoS guidelines:

• You configure QoS only on physical ports; there is no support for it at the VLAN level and EtherChannel ports.

• 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:

• Ingress queueing and aggregate policy are not supported.

• Only 32 class-maps are supported per ASIC.

• Ternary content-addressable memory (TCAM) sharing of policy-map (policer/marking) across ports is not supported. Because of this, the number of interfaces on which auto-QoS/QoS policy-map can be applied is limited.
• The same TCAM region must be used for both security Access control lists (ACLs) and ACLs used via policy map.

• Policy-maps with the `match ip dscp` command matches both IPv4 and IPv6 addresses, which limits the scale number to 16 class-maps. One TCAM entry is created for IPv4 and one TCAM entry for IPv6.

• Per ASIC, 8 TCP port comparators and 8 UDP port comparators are supported, and each `gt` (greater than)/`lt` (less than)/`neq` (not equal) operator uses 1 port comparator, and each range operator uses 2 port comparators. A policy-map with this combination affects the TCAM scale and number of interfaces to which the policy-map can be attached.

• The following restrictions apply to IPv4 ACL 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 on Layer 2 interfaces.

• Deny ACLs are not supported on QoS policy-maps.

• Policed action transmit is not supported; only exceed action drop is supported.

• You can configure QoS only on physical ports. VLAN-based QoS is not supported. You configure the QoS settings, such as classification, queueing, and scheduling, and apply the policy map to a port. When configuring QoS on a physical port, you apply a nonhierarchical policy map to a port.

### 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.
Figure 37: QoS Classification Layers in Frames and Packets

The special bits in the Layer 2 frame or a Layer 3 packet are shown in the following figure:

Layer 2 Frame Prioritization Bits
Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On ports configured as Layer 2 ISL trunks, all traffic is in ISL frames.

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 2 Frame Prioritization Bits

Layer 3 Packet Prioritization Bits

Layer 3 IP packets can carry CoS ranging from 0 to 63.

End-to-End QoS Solution Using Classification

All switches and routers that access the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class.
information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to occur closer to the edge of the network, so that the core switches and routers are not overloaded with this task.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the Diff-Serv architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple task or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control that you need over incoming and outgoing traffic.

**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 38: QoS Basic Wired Model*

**Actions at Ingress Port**

Actions at the ingress port include classifying traffic, policing, and marking:

- 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).
Actions at Egress Port

Actions at the egress port include queueing and scheduling:

- Queueing evaluates the QoS packet label and the corresponding 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.

Classification Overview

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, so no classification occurs.

During classification, the switch performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

The QoS label is based on the DSCP or the CoS value in the packet and decides the queuing and scheduling actions to perform on the packet. The label is mapped according to the trust setting and the packet type as shown in the Classification Flowchart.

You specify which fields in the frame or packet that you want to use to classify incoming traffic.

Non-IP Traffic Classification

The following table describes the non-IP traffic classification options for your QoS configuration.

<table>
<thead>
<tr>
<th>Non-IP Traffic Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust the CoS value</td>
<td>Trust the CoS value in the incoming frame (configure the port to trust CoS), and then use the configurable CoS-to-DSCP map to generate a DSCP value for the packet. Layer 2 ISL frame headers carry the CoS value in the 3 least-significant bits of the 1-byte User field. Layer 2 802.1Q frame headers carry the CoS value in the 3 most-significant bits of the Tag Control Information field. CoS values range from 0 for low priority to 7 for high priority.</td>
</tr>
</tbody>
</table>
Non-IP Traffic Classification

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust the DSCP value</td>
</tr>
<tr>
<td>Trust the DSCP value in the incoming frame. These configurations are meaningless for non-IP traffic. If you configure a port with either of these options and non-IP traffic is received, the switch assigns a CoS value and generates an internal DSCP value from the CoS-to-DSCP map. The switch uses the internal DSCP value to generate a CoS value representing the priority of the traffic.</td>
</tr>
<tr>
<td>Perform classification based on configured Layer 2 MAC ACL</td>
</tr>
<tr>
<td>Perform the classification based on a configured Layer 2 MAC access control list (ACL), which can examine the MAC source address, the MAC destination address, and other fields. If no ACL is configured, the packet is assigned 0 as the DSCP and CoS values, which means best-effort traffic. Otherwise, the policy-map action specifies a DSCP or CoS value to assign to the incoming frame.</td>
</tr>
</tbody>
</table>

After classification, the packet is sent to the policing and marking stages.

### IP Traffic Classification

The following table describes the IP traffic classification options for your QoS configuration.

**Table 53: IP Traffic Classifications**

<table>
<thead>
<tr>
<th>IP Traffic Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust the DSCP value</td>
<td>Trust the DSCP value in the incoming packet (configure the port to trust DSCP), and assign the same DSCP value to the packet. The IETF defines the 6 most-significant bits of the 1-byte ToS field as the DSCP. The priority represented by a particular DSCP value is configurable. DSCP values range from 0 to 63. You can also classify IP traffic based on IPv6 DSCP. For ports that are on the boundary between two QoS administrative domains, you can modify the DSCP to another value by using the configurable DSCP-to-DSCP-mutation map.</td>
</tr>
<tr>
<td>Trust the CoS value</td>
<td>Trust the CoS value (if present) in the incoming packet, and generate a DSCP value for the packet by using the CoS-to-DSCP map. If the CoS value is not present, use the default port CoS value.</td>
</tr>
<tr>
<td>IP standard or an extended ACL</td>
<td>Perform the classification based on a configured IP standard or an extended ACL, which examines various fields in the IP header. If no ACL is configured, the packet is assigned 0 as the DSCP and CoS values, which means best-effort traffic. Otherwise, the policy-map action specifies a DSCP or CoS value to assign to the incoming frame.</td>
</tr>
<tr>
<td>Override configured CoS</td>
<td>Override the configured CoS of incoming packets, and apply the default port CoS value to them. For IPv6 packets, the DSCP value is rewritten by using the CoS-to-DSCP map and by using the default CoS of the port. You can do this for both IPv4 and IPv6 traffic.</td>
</tr>
</tbody>
</table>
After classification, the packet is sent to the policing and marking stages.

**Access Control Lists**

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (class). You can also classify IP traffic based on IPv6 ACLs.
In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings from security ACLs:

- If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.
- If a match with a deny action is encountered, the ACL being processed is skipped, and the next ACL is processed.

**Note**  
Deny action is supported in Cisco IOS Release 3.7.4E and later releases.

- If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet, and the switch offers best-effort service to the packet.
- If multiple ACLs are configured on a port, the lookup stops after the packet matches the first ACL with a permit action, and QoS processing begins.

**Note**  
When creating an access list, note 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.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the `access-list` global configuration command; you implement Layer 2 MAC ACLs to classify non-IP traffic by using the `mac access-list extended` global configuration command.

**Classification Based on Class Maps and Policy Maps**

A class map is a mechanism that you use to name a specific traffic flow (or class) and to isolate it from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can include matching the access group defined by the ACL or matching a specific list of DSCP values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you further classify it through the use of a policy map.

A policy map specifies which traffic class to act on. Actions can include trusting the CoS or DSCP values in the traffic class; setting a specific DSCP value in the traffic class; or specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile. Before a policy map can be effective, you must attach it to a port.

You create a class map by using the `class-map` global configuration command or the `class` policy-map configuration command. You should use the `class-map` command when the map is shared among many ports. When you enter the `class-map` command, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the `match` class-map configuration command.
You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic specified in the other traffic classes configured on the policy-map) is treated as default traffic.

You create and name a policy map by using the **policy-map** global configuration command. When you enter this command, the switch enters the policy-map configuration mode. In this mode, you specify the actions to take on a specific traffic class by using the **class** or **set** policy-map configuration and policy-map class configuration commands.

The policy map can contain the **policy-class** policy-map class configuration commands, which define the policer, the bandwidth limitations of the traffic, and the action to take if the limits are exceeded.

To enable the policy map, you attach it to a port by using the **service-policy** interface configuration command.

### Policing and Marking Overview

After a packet is classified and has a DSCP-based or CoS-based QoS label assigned to it, the policing and marking process can begin.

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer decides on a packet-by-packet basis whether the packet is in or out of profile and specifies the actions on the packet. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or modifying (marking down) the assigned DSCP of the packet and allowing the packet to pass through. The configurable policed-DSCP map provides the packet with a new DSCP-based QoS label. Marked-down packets use the same queues as the original QoS label to prevent packets in a flow from getting out of order.

---

**Note**

All traffic, regardless of whether it is bridged or routed, is subjected to a policer, if one is configured. As a result, bridged packets might be dropped or might have their DSCP or CoS fields modified when they are policed and marked.

You can configure policing on a physical port. After you configure the policy map and policing actions, attach the policy to a port by using the **service-policy** interface configuration command.

### Physical Port Policing

In policy maps on physical ports, you can create individual policers. QoS applies the bandwidth limits specified in the policer separately to each matched traffic class. You configure this type of policer within a policy map by using the **policy** policy-map class configuration command.

Policing uses a token-bucket algorithm. As each frame is received by the switch, a token is added to the bucket. The bucket has a hole in it and leaks at a rate that you specify as the average traffic rate in bits per second. Each time a token is added to the bucket, the switch verifies that there is enough room in the bucket. If there is not enough room, the packet is marked as nonconforming, and the specified policer action is taken (dropped or marked down).

How quickly the bucket fills is a function of the bucket depth (burst-byte), the rate at which the tokens are removed (rate-bps), and the duration of the burst above the average rate. The size of the bucket imposes an upper limit on the burst length and limits the number of frames that can be transmitted back-to-back. If the burst is short, the bucket does not overflow, and no action is taken against the traffic flow. However, if a burst is long and at a higher rate, the bucket overflows, and the policing actions are taken against the frames in that burst.
You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the burst-byte option of the `police` policy-map class configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the `rate-bps` option of the `police` policy-map class configuration command.

*Figure 40: Policing and Marking Flowchart on Physical Ports*

---

**Queueing and Scheduling Overview**

The switch has queues at specific points to help prevent congestion.
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.

**Weighted Tail Drop**

Egress queues use an enhanced version of the tail-drop congestion-avoidance mechanism called weighted tail drop (WTD). WTD is implemented on queues to manage the queue lengths and to provide drop precedences for different traffic classifications.

As a frame is enqueued to a particular queue, WTD uses the frame’s assigned QoS label to subject it to different thresholds. If the threshold is exceeded for that QoS label (the space available in the destination queue is less than the size of the frame), the switch drops the frame.

Each queue has three threshold values. The QoS label determines which of the three threshold values is subjected to the frame. Of the three thresholds, two are configurable (explicit) and one is not (implicit).

**Figure 42: WTD and Queue Operation**

The following figure shows an example of WTD operating on a queue whose size is 1000 frames. Three drop percentages are configured: 40 percent (400 frames), 60 percent (600 frames), and 100 percent (1000 frames). These percentages indicate that up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent threshold.
In the example, CoS values 6 and 7 have a greater importance than the other CoS values, and they are assigned to the 100-percent drop threshold (queue-full state). CoS values 4 and 5 are assigned to the 60-percent threshold, and CoS values 0 to 3 are assigned to the 40-percent threshold.

Suppose the queue is already filled with 600 frames, and a new frame arrives. It contains CoS values 4 and 5 and is subjected to the 60-percent threshold. If this frame is added to the queue, the threshold will be exceeded, so the switch drops it.

**SRR Shaping and Sharing**

You can configure SRR on egress queues for sharing or for shaping.

In shaped mode, the egress queues are guaranteed a percentage of the bandwidth, and they are rate-limited to that amount. Shaped traffic does not use more than the allocated bandwidth even if the link is idle. Shaping provides a more even flow of traffic over time and reduces the peaks and valleys of bursty traffic. With shaping, the absolute value of each weight is used to compute the bandwidth available for the 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 is empty and no longer requires 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. Shaping and sharing is configured per interface. Each interface can be uniquely configured.

**Queueing and Scheduling on Egress Queues**

The following figure shows queueing and scheduling flowcharts for egress ports on the switch.
If the expedite 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.
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 {dscp1...dscp8} | threshold threshold-id dscp1...dscp8` or the `mls qos srr-queue output cos-map queue queue-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.

Shaped or Shared Mode

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.

Packet Modification

A packet is classified, policed, 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 DSCP or CoS of the received packet. However, the packet is not modified at this stage; only an indication of the assigned DSCP or CoS value is carried along.

- During policing, IP and non-IP packets can have another DSCP assigned to them (if they are out of profile and the policer specifies a markdown DSCP). Once again, the DSCP in the packet is not modified, but an indication of the marked-down value is carried along. For IP packets, the packet modification occurs
at a later stage; for non-IP packets the DSCP is converted to CoS and used for queueing and scheduling decisions.

- Depending on the QoS label assigned to a frame and the mutation chosen, the DSCP and CoS values of the frame are rewritten. If you do not configure a table map and if you configure the port to trust the DSCP of the incoming frame, the DSCP value in the frame is not changed, but the CoS is rewritten according to the DSCP-to-CoS map. 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, but the DSCP might be changed according to the CoS-to-DSCP map.

The input mutation causes the DSCP to be rewritten depending on the new value of DSCP chosen. The set action in a policy map also causes the DSCP to be rewritten.

**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 or DSCP 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.

**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 54: Default Egress Queue Configuration**

<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>80 percent</td>
<td>80 percent</td>
<td>80 percent</td>
<td>80 percent</td>
</tr>
<tr>
<td>WTD drop threshold 2</td>
<td>80 percent</td>
<td>80 percent</td>
<td>80 percent</td>
<td>80 percent</td>
</tr>
<tr>
<td>Reserved threshold</td>
<td>1000 percent</td>
<td>1000 percent</td>
<td>1000 percent</td>
<td>1000 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>
<tr>
<td>SRR shaped weights (absolute)</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
The following table shows the default CoS output queue threshold map when QoS is enabled.

**Table 55: 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>

**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).

**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>Step 1</td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```bash
configure terminal
```
<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 2**

<table>
<thead>
<tr>
<th>mls qos</th>
<th>Enables QoS globally. QoS operates with the default settings described in the related topic sections below.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# mls qos</td>
<td></td>
</tr>
</tbody>
</table>

**Note** To disable QoS, use the `no mls qos` global configuration command.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show mls qos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show mls qos</td>
<td>Verifies the QoS configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>copy running-config startup-config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Configuring Classification Using Port Trust States**

These sections describe how to classify incoming traffic by using port trust states.

**Note** Depending on your network configuration, you must perform one or more of these tasks in this module or one or more of the tasks in the Configuring a QoS Policy.

**Configuring the Trust State on Ports Within the QoS Domain**

Packets entering a QoS domain are classified at the edge of the QoS domain. When the packets are classified at the edge, the switch port within the QoS domain can be configured to one of the trusted states because there is no need to classify the packets at every switch within the QoS domain.
Figure 44: Port Trusted States on Ports Within the QoS Domain

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. mls qos trust [cos | dscp]
4. end
5. show mls qos interface
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>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>Specifies the port to be trusted, and enters interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the CoS Value for an Interface

QoS assigns the CoS value specified with the `mls qos cos` interface configuration command to untagged frames received on trusted and untrusted ports.

Beginning in privileged EXEC mode, follow these steps to define the default CoS value of a port or to assign the default CoS to all incoming packets on the port.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td>Configures the port trust state. By default, the port is not trusted. If no keyword is specified, the default is <code>dscp</code>. The keywords have these meanings:</td>
</tr>
<tr>
<td><strong>Step 3</strong> `mls qos trust [cos</td>
<td>dscp]<code>**Example:**</code>Switch(config-if)# mls qos trust cos`</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>end</code> <strong>Example:</strong> <code>Switch(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>show mls qos interface</code> <strong>Example:</strong> <code>Switch# show mls qos interface</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>copy running-config startup-config</code> <strong>Example:</strong> <code>Switch# copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. mls qos cos {default-cos | override }
4. end
5. show mls qos interface
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 the global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Example:</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet0/2</td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures the default CoS value for the port.</td>
</tr>
<tr>
<td>mls qos cos {default-cos</td>
<td>override }</td>
</tr>
<tr>
<td>Switch(config-if)# mls qos cos override</td>
<td></td>
</tr>
</tbody>
</table>

- For *default-cos*, specify a default CoS value to be assigned to a port. If the packet is untagged, the default CoS value becomes the packet CoS value. The CoS range is 0 to 7. The default is 0.

- Use the *override* keyword to override the previously configured trust state of the incoming packet and to apply the default port CoS value to the port on all incoming packets. By default, CoS override is disabled. Use the *override* keyword when all incoming packets on specified ports deserve higher or lower priority than packets entering from other ports. Even if a port was previously set to trust DSCP or CoS, this command overrides the previously configured trust state, and all the incoming CoS values are assigned the default CoS value configured with this command. If an incoming packet is tagged, the CoS value of the packet is modified with the default CoS of the port at the ingress port.

**Note** To return to the default setting, use the **no mls qos cos {default-cos | override}** interface configuration command.
### Configuring a Trusted Boundary to Ensure Port Security

In a typical network, you connect a Cisco IP Phone to a switch port and cascade devices that generate data packets from the back of the telephone. The Cisco IP Phone guarantees the voice quality through a shared data link by marking the CoS level of the voice packets as high priority (CoS = 5) and by marking the data packets as low priority (CoS = 0). Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the class of service (CoS) 3-bit field, which is the priority of the packet.

For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch should be trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the `mls qos trust cos` interface configuration command, you configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port. Use the `mls qos trust dscp` interface configuration command to configure a routed port to which the telephone is connected to trust the DSCP labels of all traffic received on that port.

With the trusted setting, you also can use the trusted boundary feature to prevent misuse of a high-priority queue if a user bypasses the telephone and connects the PC directly to the switch. Without trusted boundary, the CoS labels generated by the PC are trusted by the switch (because of the trusted CoS setting). By contrast, trusted boundary uses CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a switch port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the switch port and prevents misuse of a high-priority queue. Note that the trusted boundary feature is not effective if the PC and Cisco IP Phone are connected to a hub that is connected to the switch.

### SUMMARY STEPS

1. `configure terminal`
2. `cdp run`
3. `interface interface-id`
4. `cdp enable`
5. Use one of the following:
   • `mls qos trust cos`
   • `mls qos trust dscp`

6. `mls qos trust device cisco-phone`

7. `end`

8. `show mls qos interface`

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>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the 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>Step 2</td>
<td><code>cdp run</code></td>
<td>Enables CDP globally. By default, CDP is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# cdp run</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>interface interface-id</code></td>
<td>Specifies the port connected to the Cisco IP Phone, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Validates the port connected to the Cisco IP Phone.</td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet0/1</code></td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>cdp enable</code></td>
<td>Enables CDP on the port. By default, CDP is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# cdp enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Use one of the following:</td>
<td>Configures the switch port to trust the CoS value in traffic received from the Cisco IP Phone.</td>
</tr>
<tr>
<td></td>
<td>• <code>mls qos trust cos</code></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>• <code>mls qos trust dscp</code></td>
<td>Configures the routed port to trust the DSCP value in traffic received from the Cisco IP Phone.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>By default, the port is not trusted.</td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# mls qos trust cos</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>mls qos trust device cisco-phone</code></td>
<td>Specifies that the Cisco IP Phone is a trusted device.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>You cannot enable both trusted boundary and auto-QoS (<code>auto qos voip interface configuration command</code>) at the same time; they are mutually exclusive.</td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# mls qos trust</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>
<tr>
<td><code>device cisco-phone</code></td>
<td><strong>Purpose</strong>: To disable the trusted boundary feature, use the <code>no mls qos trust device</code> interface configuration command. <strong>Note</strong>: Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Step 7</strong>: Returns to privileged EXEC mode. Example: Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Step 8</strong>: Verifies your entries. Example: Switch# show mls qos interface</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>Step 9</strong>: (Optional) Saves your entries in the configuration file. Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Enabling DSCP Transparency Mode**

The switch supports the DSCP transparency feature. It affects only the DSCP field of a packet at egress. By default, DSCP transparency is disabled. The switch modifies the DSCP field in an incoming packet, and the DSCP field in the outgoing packet is based on the quality of service (QoS) configuration, including the port trust setting, policing, and marking.

If DSCP transparency is enabled by using the `no mls qos rewrite ip dscp` command, the switch does not modify the DSCP field in the incoming packet, and the DSCP field in the outgoing packet is the same as that in the incoming packet.

Regardless of the DSCP transparency configuration, the switch modifies the internal DSCP value of the packet, which the switch uses to generate a class of service (CoS) value that represents the priority of the traffic. The switch also uses the internal DSCP value to select an egress queue and threshold.

**SUMMARY STEPS**

1. configure terminal
2. mls qos
3. `no mls qos rewrite ip dscp`
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>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>mls qos</code></td>
<td>Enables QoS globally.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>mls qos</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>no mls qos rewrite ip dscp</code></td>
<td>Enables DSCP transparency. The switch is configured to not modify the DSCP field of the IP packet.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# <code>no mls qos rewrite ip dscp</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: Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>show mls qos interface [interface-id]</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# <code>show mls qos interface gigabitethernet0/1</code></td>
<td></td>
</tr>
<tr>
<td>6</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>Example: Switch# <code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### DSCP Transparency Mode

To configure the switch to modify the DSCP value based on the trust setting or on an ACL by disabling DSCP transparency, use the `mls qos rewrite ip dscp` global configuration command.

If you disable QoS by using the `no mls qos` global configuration command, the CoS and DSCP values are not changed (the default QoS setting).

If you enter the `no mls qos rewrite ip dscp` global configuration command to enable DSCP transparency and then enter the `mls qos trust [cos | dscp]` interface configuration command, DSCP transparency is still enabled.
For Catalyst 2960-L switches, DSCP transparency is disabled by default.

**Configuring the DSCP Trust State on a Port Bordering Another QoS Domain**

If you are administering two separate QoS domains between which you want to implement QoS features for IP traffic, you can configure the switch ports bordering the domains to a DSCP-trusted state. The receiving port accepts the DSCP-trusted value and avoids the classification stage of QoS. If the two domains use different DSCP values, you can configure the DSCP-to-DSCP-mutation map to translate a set of DSCP values to match the definition in the other domain.

*Figure 45: DSCP-Trusted State on a Port Bordering Another QoS Domain*

Beginning in privileged EXEC mode, follow these steps to configure the DSCP-trusted state on a port and modify the DSCP-to-DSCP-mutation map. To ensure a consistent mapping strategy across both QoS domains, you must perform this procedure on the ports in both domains.

**SUMMARY STEPS**

1. configure terminal
2. mls qos map dscp-mutation in-dscp to out-dscp
3. interface interface-id
4. mls qos trust dscp
5. end
6. show mls qos maps dscp-mutation
7. copy running-config startup-config

**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 the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</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>Switch# configure terminal</td>
<td>Modifies the DSCP-to-DSCP-mutation map. The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> mls qos map dscp-mutation in-dscp to out-dscp <strong>Example:</strong> Switch(config)# mls qos map dscp-mutation 10 11 12 13 to 30</td>
<td>For <em>in-dscp</em>, enter up to eight DSCP values separated by spaces. Then enter the <em>to</em> keyword. For <em>out-dscp</em>, enter a single DSCP value. The DSCP range is 0 to 63.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id <strong>Example:</strong> Switch(config)# interface gigabitethernet0/2</td>
<td>Specifies the port to be trusted, and enter interface configuration mode. Valid interfaces include physical ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mls qos trust dscp <strong>Example:</strong> Switch(config-if)# mls qos trust dscp</td>
<td>Configures the ingress port as a DSCP-trusted port. By default, the port is not trusted. <strong>Note</strong> To return a port to its non-trusted state, use the <em>no mls qos trust</em> interface configuration command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end <strong>Example:</strong> Switch(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show mls qos maps dscp-mutation <strong>Example:</strong> Switch# show mls qos maps dscp-mutation</td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config <strong>Example:</strong> Switch# copy-running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file. <strong>Note</strong> To return a port to its non-trusted state, use the <em>no mls qos trust</em> interface configuration command. To return to the default DSCP-to-DSCP-mutation map values, use the <em>no mls qos map dscp-mutation dscp-mutation-name</em> global configuration command.</td>
<td></td>
</tr>
</tbody>
</table>
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.

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 {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><strong>Purpose</strong></td>
</tr>
<tr>
<td>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></td>
<td><strong>Create an IP standard ACL, repeating the command as many times as necessary.</strong></td>
</tr>
</tbody>
</table>
| access-list access-list-number {permit} source [source-wildcard] | • For access-list-number, enter the access list number. The range is 1 to 99 and 1300 to 1999.  
  • Use the permit keyword to permit a certain type of traffic if the conditions are matched. |
| Example: Switch(config)# access-list 1  
  permit 192.2.255.0 1.1.1.255 | **DETAILED STEPS** |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For <em>source</em>, enter the network or host from which the packet is being sent. You can use the <em>any</em> keyword as an abbreviation for 0.0.0.0 255.255.255.255.</td>
<td></td>
</tr>
<tr>
<td>• (Optional) For <em>source-wildcard</em>, 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.</td>
<td></td>
</tr>
</tbody>
</table>

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.

**Note** To delete an access list, use the `no access-list access-list-number` global configuration command.

---

### 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.

---

### 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* 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> 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> access-list access-list-number permit protocol source source-wildcard destination destination-wildcard</td>
<td>Creates an IP extended ACL, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# access-list 100 permit ip any any dscp 32</td>
<td></td>
</tr>
<tr>
<td>• For access-list-number, enter the access list number. The range is 100 to 199 and 2000 to 2699.</td>
<td></td>
</tr>
<tr>
<td>• Use the permit keyword to permit a certain type of traffic if the conditions are matched.</td>
<td></td>
</tr>
<tr>
<td>• For protocol, enter the name or number of an IP protocol. Use the question mark (?) to see a list of available protocol keywords.</td>
<td></td>
</tr>
<tr>
<td>• For source, enter the network or host from which the packet is being sent. You specify this by using dotted decimal notation, by using the any keyword as an abbreviation for source 0.0.0.0 source-wildcard 255.255.255.255, or by using the host keyword for source 0.0.0.0.</td>
<td></td>
</tr>
<tr>
<td>• For source-wildcard, enter the wildcard bits by placing ones in the bit positions that you want to ignore. You specify the wildcard by using dotted decimal notation, by using the any keyword as an abbreviation for source 0.0.0.0 source-wildcard 255.255.255.255, or by using the host keyword for source 0.0.0.0.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To delete an access list, use the no access-list access-list-number global configuration command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
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. {permit|deny} 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]
4. end
5. show ipv6 access-list
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></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ipv6 access-list access-list-name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ipv6 access-list ipv6_Name_ACL</td>
<td>Creates an IPv6 ACL and enters IPv6 access-list configuration mode.</td>
</tr>
<tr>
<td>Accesses list names cannot contain a space or quotation mark or begin with a numeric.</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Step 3 | \{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] |
| --- | --- |
| **Example:** | Switch(config-ipv6-acl)# permit ip host 10::1 host 11::2 host |

### Purpose

Enters `permit` to permit the packet if conditions are matched. These are the conditions:

- 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.

  - 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 permit condition, 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 permit condition, 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 match the source port. If the operator follows the `destination-ipv6-prefix/ prefix-length` argument, it must match the destination port.

  - (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.

  - (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.

### Step 4

<table>
<thead>
<tr>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
</table>
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 | Enters global configuration mode. |

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2**
mac access-list extended name
Example:
Switch(config)# mac access-list extended maclist1 | Creates a Layer 2 MAC ACL by specifying the name of the list. 
After entering this command, the mode changes to extended MAC ACL configuration. |
Creating a Layer 2 MAC ACL for Non-IP Traffic

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>To delete an access list, use the <strong>no mac access-list extended access-list-name</strong> global configuration command.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

```
{permit | deny} {host src-MAC-addr mask | any | host dst-MAC-addr | dst-MAC-addr mask} [type mask]
```

**Example:**

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

Specifies the type of traffic to permit or deny if the conditions are matched, entering the command as many times as necessary.

- For src-MAC-addr, enter the MAC address of the host from 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.

- 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.

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.

**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:**

(Optional) Saves your entries in the configuration file.
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 or DSCP values. The match criterion is defined with one match statement entered within the class-map configuration mode.

**Note**
You can also create class maps during policy map creation by using the `class` policy-map configuration command.

**SUMMARY STEPS**

1. `configure terminal`
2. Use one of the following:
   - `access-list access-list-number {permit} source [source-wildcard]`
   - `access-list access-list-number {permit} protocol source [source-wildcard] destination [destination-wildcard]`
   - `ipv6 access-list access-list-name {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]`
   - `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] class-map-name`
4. `match {access-group acl-index-or-name | ip dscp dscp-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><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters the 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

**Command or Action**  

**Step 2**  
Use one of the following:

- `access-list access-list-number {permit} source [source-wildcard]`
- `access-list access-list-number {permit} source [source-wildcard] destination [destination-wildcard]`
- `ipv6 access-list access-list-name {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]`
- `mac access-list extended name {permit | deny} {host src-MAC-addr mask | any | host dst-MAC-addr | dst-MAC-addr mask} [type mask]`

**Example:**

```
Switch(config)# access-list 103 permit ip any any dscp 10
```

**Step 3**

**class-map [match-all] class-map-name**

**Example:**

```
Switch(config)# class-map class1
```

**Step 4**

**match {access-group acl-index-or-name | ip dscp dscp-list}**

**Example:**

```
Switch(config-cmap)# match ip dscp 10 11 12
```

---

**Purpose**

**Step 2**

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.

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.

**Example:**

```
Switch(config)# access-list 103 permit ip any any dscp 10
```
### 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 or DSCP values in the traffic class; setting a specific DSCP 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.
- mls qos must be enabled in global configuration mode.
- If you enter or have used the `set ip dscp` command, the switch changes this command to `set dscp` in its 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* For <code>ip dscp dscp-list</code>, 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>Note</td>
<td>To remove a match criterion, use the `no match {access-group acl-index-or-name</td>
</tr>
</tbody>
</table>

**Step 5**

**end**

**Example:**

```
Switch(config-cmap)# end
```

Returns to privileged EXEC mode.

**Step 6**

**show class-map**

**Example:**

```
Switch# show class-map
```

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.
• 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 class-map-name`  
3. `policy-map policy-map-name`  
4. `class [class-map-name | class-default]`  
5. `set dscp new-dscp`  
6. `police rate-bps burst-byte [exceed-action {drop}]`  
7. `exit`  
8. `exit`  
9. `interface interface-id`  
10. `service-policy input policy-map-name`  
11. `end`  
12. `show policy-map [policy-map-name [class class-map-name]]`  
13. `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>
<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 class-map-name` |  |
| **Example:** | |
| Switch(config)# class-map ipclass1 |  |

| **Step 3** | Creates a policy map by entering the policy map name, and enters policy-map configuration mode. |
| `policy-map policy-map-name` |  |
| **Example:** | |
| Switch(config-cmap)# policy-map flowit |  |

**Note** To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command.

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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>**class [class-map-name</td>
<td>class-default]**</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Switch(config-pmap)# <strong>class ipclass1</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>set dscp new-dscp</strong></td>
<td>Classifies IP traffic by setting a new value in the packet.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Switch(config-pmap-c)# <strong>set dscp 45</strong></td>
</tr>
<tr>
<td>6</td>
<td><strong>police rate-bps burst-byte [exceed-action {drop}]</strong></td>
<td>Defines a policer for the classified traffic. By default, no policer is defined.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Switch(config-pmap-c)# <strong>police 100000 80000 exceed-action drop</strong></td>
</tr>
<tr>
<td>7</td>
<td><strong>exit</strong></td>
<td>Returns to policy map configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></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>Switch(config-pmap-c)# exit</td>
<td>Returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Specifies the port to attach to the policy map, and enters interface configuration mode. Valid interfaces include physical ports.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config-pmap)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> interface interface-id</td>
<td>Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet0/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> service-policy input policy-map-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>To remove the policy map and port association, use the no service-policy input policy-map-name interface configuration command.</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# service-policy input flowit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> 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-if)# end</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> show policy-map [policy-map-name [class class-map-name]]</td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# show policy-map</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> 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>Switch# copy-running-config startup-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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?
• 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?

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.

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. Default number of queues is 4. You can increase it to 8 using the `mls qos srr-queue output queues 8` command.

Note

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>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**

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`

**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.
- 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 `dscp1...dscp8`, enter up to eight values, and separate each value with a space. The range is 0 to 63.
- 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 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**

`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.
### Purpose

**Command or Action**

- 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

**end**

**Example:**

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

Returns to privileged EXEC mode.

### Step 5

**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).

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).

### 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.

---

**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**
### Configuring SRR Shaped Weights on Egress Queues

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>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>srr-queue bandwidth shape weight1 weight2 weight3 weight4</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>show mls qos interface interface-id queueing</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
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>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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> interface interface-id</td>
<td>Specifies the port of the outbound traffic, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface</td>
<td></td>
</tr>
<tr>
<td>gigabitethernet0/1</td>
<td></td>
</tr>
</tbody>
</table>
### 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**

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></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 <strong>no srr-queue bandwidth share</strong> interface configuration command.</td>
</tr>
<tr>
<td><code>srr-queue bandwidth share weight1 weight2 weight3 weight4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-id)# srr-queue bandwidth share 1 2 3 4</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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-id)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>show mls qos interface interface-id queuing</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# show mls qos interface interface_id queuing</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file. To return to the default setting, use the <strong>no srr-queue bandwidth share</strong> interface configuration command.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></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>
# Configuring the Egress Expedite Queue

## 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 | mls qos  
Example:  
Switch(config)# mls qos | Enables QoS on a switch. |
| Step 3 | interface interface-id  
Example:  
Switch(config)# interface gigabitethernet 0/1 | Specifies the egress port, and enters interface configuration mode. |
| Step 4 | priority-queue out  
Example:  
Switch(config-if)# 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. |
| Step 5 | end  
Example:  
Switch(config-if)# 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 | (Optional) Saves your entries in the configuration file.  
To disable the egress expedite queue, use the no priority-queue out interface configuration command. |
### 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>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>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface interface-id</code></td>
<td>Specifies the port to be rate-limited, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>srr-queue bandwidth limit weight1</code></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# <code>srr-queue bandwidth limit 80</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>To return to the default setting, use the <code>no srr-queue bandwidth limit</code> interface configuration command.</td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring Standard QoS

**Table 56: 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] [policers</td>
<td>queueing</td>
</tr>
<tr>
<td>`show mls qos maps [cos-output-q</td>
<td>dscp-mutation ]`</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 so that incoming DSCP values 10 to 13 are mapped to DSCP 30:

Switch(config)# mls qos map dscp-mutation
10 11 12 13 to 30
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# end

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)
```

**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 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)# exit
Switch(config)# Class-map cm-2
Switch(config-cmap)# match ip dscp 20
Switch(config-cmap)# exit
Switch(config)# Policy-map pml
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
```
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)# ip 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-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)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
```

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:

```
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)# set dscp cs1
Switch(config-pmap-c)# police 1000000 8000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# interface gigabitethernet 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.

```
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)# 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-pmap)# class macclass2 maclist2
Switch(config-pmap-c)# set dscp 45
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 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:

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 pml
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-pmap)# exit
Switch(config)# interface G0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# service-policy input pml

Examples: Configuring DSCP-to-DSCP Mutation Maps

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)# mls qos map dscp-mutation 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation
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 10 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 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.

**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 gigabitethernet 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 gigabitethernet 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 gigabitethernet 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 gigabitethernet 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.

Where to Go Next

Review the auto-QoS documentation to see if you can use these automated capabilities for your QoS configuration.

Feature History and Information for QoS

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Feature History and Information for QoS
Configuring AutoQoS

- Finding Feature Information, on page 439
- Prerequisites for Auto-QoS, on page 439
- Restrictions for Auto-QoS, on page 440
- Information about Configuring Auto-QoS, on page 440
- How to Configure Auto-QoS, on page 444
- Monitoring Auto-QoS, on page 448
- Configuration Examples for Auto-Qos, on page 449
- Where to Go Next for Auto-QoS, on page 453
- Additional References for Auto-QoS, on page 453
- Feature History and Information for Auto-QoS, on page 454

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 Auto-QoS

Before configuring standard QoS or auto-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. Is the traffic 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.
Restrictions for Auto-QoS

The following are restrictions for automatic QoS (auto-QoS):

- Ternary content-addressable memory (TCAM) sharing of policy-map (policer/marking) across ports is not supported. Because of this, the number of interfaces on which auto-QoS/QoS policy-map can be applied is limited.

- The same TCAM region must be used for both security Access control lists (ACLs) and ACLs used via policy map.

- Policy-maps with the `match ip dscp` command matches both IPv4 and IPv6 addresses, which limits the scale number to 16 class-maps. One TCAM entry is created for IPv4 and one TCAM entry for IPv6.

- Per ASIC, 8 TCP port comparators and 8 UDP port comparators are supported, and each gt (greater than)/lt (less than)/neq (not equal) operator uses 1 port comparator, and each range operator uses 2 port comparators. A policy-map with this combination affects the TCAM scale and number of interfaces to which the policy-map can be attached.

- The following restrictions apply to IPv4 ACL 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 on Layer 2 interfaces.

- Deny ACLs are not supported on QoS policy-maps.

Information about Configuring Auto-QoS

Auto-QoS Overview

You can use the auto-QoS feature to simplify the deployment of QoS features. Auto-QoS determines the network design and enables QoS configurations so that the switch can prioritize different traffic flows. It uses the egress queues instead of using the default (disabled) QoS behavior. The switch offers best-effort service to each packet, regardless of the packet contents or size, and sends it from a single queue.

When you enable auto-QoS, it automatically classifies traffic based on the traffic type and ingress packet label. The switch uses the classification results to choose the appropriate egress queue.

You can use auto-QoS commands to identify ports connected to the following Cisco devices:

- Cisco IP Phones
- Devices running the Cisco SoftPhone application
- Cisco TelePresence
- Cisco IP Camera
- Cisco digital media player
You also use the auto-QoS commands to identify ports that receive trusted traffic through an uplink. Auto-QoS then performs these functions:

- Detects the presence or absence of auto-QoS devices through conditional trusted interfaces.
- Configures QoS classification
- Configures egress queues

**Auto-QoS Compact Overview**

When you enter an auto-QoS command, the switch displays all the generated commands as if the commands were entered from the CLI. You can use the auto-QoS compact feature to hide the auto-QoS generated commands from the running configuration. This would make it easier to comprehend the running-configuration and also help to increase efficient usage of memory.

**Generated Auto-QoS Configuration**

By default, auto-QoS is disabled on all ports. Packets are not modified--the CoS, DSCP and IP precedence values in the packet are not changed.

When you enable the auto-QoS feature on the first port of the interface:

- Ingress packet label is used to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.
- QoS is globally enabled (mls qos global configuration command), and other global configuration commands are automatically generated. (See Examples: Global Auto-QoS Configuration, on page 449).
- Switch enables the trusted boundary feature and uses the Cisco Discovery Protocol (CDP) to detect the presence of a supported device.
- Policing is used to determine whether a packet is in or out of profile and specifies the action on the packet.

**VoIP Device Specifics**

The following activities occur when you issue these auto-QoS commands on a port:

- When you enter the `auto qos voip cisco-phone` command on a port at the network edge connected to a Cisco IP Phone, the switch enables the trusted boundary feature. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. When there is no Cisco IP Phone, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to the traffic matching the policy-map classification before the switch enables the trust boundary feature.

- When you enter the `auto qos voip cisco-softphone` interface configuration command on a port at the network edge that is connected to a device running the Cisco SoftPhone, the switch uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0.

- When you enter the `auto qos voip trust` interface configuration command on a port connected to the network interior, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).
### Enhanced Auto-QoS for Video, Trust, and Classification

Auto-QoS is enhanced to support video. Automatic configurations are generated that classify and trust traffic from Cisco TelePresence systems and Cisco IP cameras.

#### Auto-QoS Configuration Migration

Auto-QoS configuration migration from legacy auto-QoS to enhanced auto-QoS occurs when:

- A switch is booted with a 12.2(55)SE image and QoS is not enabled.
  
  Any video or voice trust configuration on the interface automatically generates enhanced auto-QoS commands.

- A switch is enabled with QoS, these guidelines take effect:
  
  - If you configure the interface for conditional trust on a voice device, only the legacy auto-QoS VoIP configuration is generated.
  
  - If you configure the interface for conditional trust on a video device, the enhanced auto-QoS configuration is generated.
  
  - If you configure the interface with classification or conditional trust based on the new interface auto-QoS commands, enhanced auto-QoS configuration is generated.

- Auto-QoS migration happens after a new device is connected when the `auto qos srnd4` global configuration command is enabled.

---

<table>
<thead>
<tr>
<th>Table 57: Traffic Types, Packet Labels, and Queues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table 57: Traffic Types, Packet Labels, and Queues</strong></td>
</tr>
<tr>
<td><strong>Traffic</strong></td>
</tr>
<tr>
<td>VoIP Data Traffic</td>
</tr>
<tr>
<td>DSCP value</td>
</tr>
<tr>
<td>CoS value</td>
</tr>
<tr>
<td>CoS-to-Egress queue map</td>
</tr>
</tbody>
</table>

- When you enable auto-QoS by using the `auto qos voip cisco-phone`, the `auto qos voip cisco-softphone`, or the `auto qos voip trust` interface configuration command, the switch automatically generates a QoS configuration based on the traffic type and ingress packet label and applies the commands listed in Examples: Global Auto-QoS Configuration, on page 449 to the port.

---

**Note**

If an interface previously configured with legacy auto-QoS migrates to enhanced auto-QoS, voice commands and configuration are updated to match the new global QoS commands.

Auto-QoS configuration migration from enhanced auto-QoS to legacy auto-QoS can occur only when you disable all existing auto-QoS configurations from the interface.
Auto-QoS Configuration Guidelines

Before configuring auto-QoS, you should be aware of this information:

- After auto-QoS is enabled, do not modify a policy map that includes AutoQoS in its name. If you need to modify the policy map, make a copy of it, and change the copied policy map. To use this new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map to the interface.

- To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. If necessary, you can fine-tune the QoS configuration, but we recommend that you do so only after the auto-QoS configuration is completed.

- You can enable auto-QoS on static, dynamic-access, voice VLAN access, and trunk ports.

- By default, the CDP is enabled on all ports. For auto-QoS to function properly, do not disable CDP.

Auto-QoS VoIP Considerations

Before configuring auto-QoS for VoIP, you should be aware of this information:

- Auto-QoS configures the switch for VoIP with Cisco IP Phones on nonrouted and routed ports. Auto-QoS also configures the switch for VoIP with devices running the Cisco SoftPhone application.

  Note
  When a device running Cisco SoftPhone is connected to a nonrouted or routed port, the switch supports only one Cisco SoftPhone application per port.

- When enabling auto-QoS with a Cisco IP Phone on a routed port, you must assign a static IP address to the IP phone.

- This release supports only Cisco IP SoftPhone Version 1.3(3) or later.

- Connected devices must use Cisco Call Manager Version 4 or later.

Auto-QoS Enhanced Considerations

Auto-QoS is enhanced to support video. Automatic configurations are generated that classify and trust traffic from Cisco TelePresence systems and Cisco IP cameras.

Before configuring auto-QoS enhanced, you should be aware of this information:

- The auto qos srnd4 global configuration command is generated as a result of enhanced auto-QoS configuration.

Effects of Auto-QoS on Running Configuration

When auto-QoS is enabled, the auto qos interface configuration commands and the generated global configuration are added to the running configuration.

The switch applies the auto-QoS-generated commands as if the commands were entered from the CLI. An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions may occur without warning. If all the generated commands are
successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands are not applied, the previous running configuration is restored.

**Effects of Auto-Qos Compact on Running Configuration**

If auto-QoS compact is enabled:

- Only the auto-QoS commands entered from the CLI are displayed in running-config.
- The generated global and interface configurations are hidden.
- When you save the configuration, only the auto-qos commands you have entered are saved (and not the hidden configuration).
- When you reload the switch, the system detects and re-executes the saved auto-QoS commands and the AutoQoS SRND4.0 compliant config-set is generated.

**Note**

Do not make changes to the auto-QoS-generated commands when auto-QoS compact is enabled, because user-modifications are overridden when the switch reloads.

When auto-qos global compact is enabled:

- `show derived-config` command can be used to view hidden AQC derived commands.
- AQC commands will not be stored to memory. They will be regenerated every time the switch is reloaded.
- When compaction is enabled, auto-qos generated commands should not be modified.
- If the interface is configured with auto-QoS and if AQC needs to be disabled, auto-qos should be disabled at interface level first.

**How to Configure Auto-QoS**

**Configuring Auto-QoS**

**Enabling Auto-QoS**

For optimum QoS performance, enable auto-QoS on all the devices in your network.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. Use one of the following:
   
   - `auto qos voip {cisco-phone | cisco-softphone | trust}`
• auto qos video \{cts | ip-camera | media-player\}
• auto qos classify [police]
• auto qos trust \{cos | dscp\}

4. exit
5. interface interface-id
6. auto qos trust
7. end
8. show auto qos interface interface-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>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>Specifies the port that is connected to a video device or the uplink port that is connected to another trusted switch or router in the network interior, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Use one of the following:</td>
<td>Enables auto-QoS for VoIP.</td>
</tr>
<tr>
<td></td>
<td>• auto qos voip {cisco-phone</td>
<td>cisco-softphone</td>
</tr>
<tr>
<td></td>
<td>• auto qos video {cts</td>
<td>ip-camera</td>
</tr>
<tr>
<td></td>
<td>• auto qos classify [police]</td>
<td>• trust—The uplink port is connected to a trusted switch or router, and the VoIP traffic classification in the ingress packet is trusted.</td>
</tr>
<tr>
<td></td>
<td>• auto qos trust {cos</td>
<td>dscp}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# auto qos trust dscp</td>
<td></td>
</tr>
</tbody>
</table>

Enables auto-QoS labels of incoming packets are trusted only when the system is detected.

Enables auto-QoS for classification.
### Enabling Auto-QoS Compact

To enable auto-QoS compact, enter this command:

**SUMMARY STEPS**

1. configure terminal
2. auto qos global compact

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| • police — Policing is set up by defining the QoS policy maps and applying them to ports (port-based QoS). Enables auto-QoS for trusted interfaces.  
  • cos — Class of service.  
  • dscp — Differentiated Services Code Point.  
  • <cr> — Trust interface. | |

| Step 4 | exit  
Example:  
Switch(config-if)# exit | Returns to global configuration mode. |
|---------|---------|
| Step 5 | interface interface-id  
Example:  
Switch(config)# interface gigabitethernet 0/1 | Specifies the switch port identified as connected to a trusted switch or router, and enters interface configuration mode. |
| Step 6 | auto qos trust  
Example:  
Switch(config-if)# auto qos trust | Enables auto-QoS on the port, and specifies that the port is connected to a trusted router or switch. |
| Step 7 | end  
Example:  
Switch(config-if)# end | Returns to privileged EXEC mode. |
| Step 8 | show auto qos interface interface-id  
Example:  
Switch# show auto qos interface gigabitethernet 0/1 | Verifies your entries.  
This command displays the auto-QoS command on the interface on which auto-QoS was enabled. You can use the show running-config privileged EXEC command to display the auto-QoS configuration and the user modifications. |
### 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 the global configuration mode. |
| **Step 2**
  - auto qos global compact
  - Example:
    - Switch(config)# auto qos global compact
| Enables auto-Qos compact and generates (hidden) the global configurations for auto-QoS. |

You can then enter the auto-QoS command you want to configure in the interface configuration mode and the interface commands that the system generates are also hidden.

To display the auto-QoS configuration that has been applied, use these the privileged EXEC commands:

- `show derived-config`
- `show policy-map`
- `show access-list`
- `show class-map`
- `show auto-qos`
- `show policy-map interface`
- `show ip access-lists`

These commands will have keyword "AutoQos-".

### What to do next

To disable auto-QoS compact, remove auto-Qos instances from all interfaces by entering the `no` form of the corresponding auto-QoS commands and then enter the `no auto qos global compact` global configuration command.

### Troubleshooting Auto-QoS

To troubleshoot auto-QoS, use the `debug auto qos` privileged EXEC command. For more information, see the `debug auto qos` command in the command reference for this release.

To disable auto-QoS on a port, use the `no` form of the `auto qos` command interface configuration command, such as `no auto qos voip`. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the `no auto qos voip` command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).
## Monitoring Auto-QoS

Table 58: Commands for Monitoring Auto-QoS

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show auto qos [interface [interface-type]]</code></td>
<td>Displays the initial auto-QoS configuration. You can compare the <code>show auto qos</code> and the <code>show running-config</code> command output to identify the user-defined QoS settings.</td>
</tr>
<tr>
<td>`show mls qos [ interface</td>
<td>maps]`</td>
</tr>
<tr>
<td>`show mls qos interface [interface-type</td>
<td>queueing</td>
</tr>
<tr>
<td>`show mls qos maps [ cos-output-q</td>
<td>dscp-mutation</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Displays information about the QoS configuration that might be affected by auto-QoS. You can compare the <code>show auto qos</code> and the <code>show running-config</code> command output to identify the user-defined QoS settings.</td>
</tr>
</tbody>
</table>
# Configuration Examples for Auto-Qos

## Examples: Global Auto-QoS Configuration

The following table describes the automatically generated commands for auto-QoS and enhanced auto-QoS by the switch.

*Table 59: Generated Auto-QoS Configuration*

<table>
<thead>
<tr>
<th>Description</th>
<th>Automatically Generated Command (voip)</th>
</tr>
</thead>
</table>
| The switch automatically maps CoS values to an egress queue and to a threshold ID. | Switch(config)# no mls qos srr-queue output cos-map  
Switch(config)# mls qos srr-queue output cos-map queue 1 threshold 1 4  
Switch(config)# mls qos srr-queue output cos-map queue 2 threshold 1 2 6 7 6 7  
Switch(config)# mls qos srr-queue output cos-map queue 3 threshold 2 3 4  
Switch(config)# mls qos srr-queue output cos-map queue 4 threshold 2 1 |
The switch automatically maps DSCP values to an egress queue and to a threshold ID.

<table>
<thead>
<tr>
<th>Description</th>
<th>Automatically Generated Command (voip)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Switch(config)# no mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 1 threshold 2</td>
</tr>
<tr>
<td></td>
<td>32 33 40 41 42 43 44 45</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 1 threshold 2</td>
</tr>
<tr>
<td></td>
<td>46 47</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 2 threshold 1</td>
</tr>
<tr>
<td></td>
<td>16 17 18 19 20 21 22 23</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 2 threshold 1</td>
</tr>
<tr>
<td></td>
<td>26 27 28 29 30 31 34 35</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 2 threshold 1</td>
</tr>
<tr>
<td></td>
<td>36 37 38 39</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 2 threshold 2</td>
</tr>
<tr>
<td></td>
<td>24 48 49 50 51 52 53 54</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 2 threshold 2</td>
</tr>
<tr>
<td></td>
<td>55 56 57 58 59 60 61 62</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 2 threshold 2</td>
</tr>
<tr>
<td></td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 3 threshold 1</td>
</tr>
<tr>
<td></td>
<td>0 1 2 3 4 5 6 7</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# mls qos srr-queue</td>
</tr>
<tr>
<td></td>
<td>output dscp-map queue 4 threshold 1</td>
</tr>
<tr>
<td></td>
<td>8 9 10 11 12 13 14 15</td>
</tr>
</tbody>
</table>

Examples: Auto-QoS Generated Configuration For Enhanced Video, Trust, and Classify Devices

If you entered the following enhanced auto-QoS commands, the switch configures a CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value):

- auto qos video cts
- auto qos video ip-camera
- auto qos video media-player
- auto qos trust
- auto qos trust cos
- auto qos trust dscp

If you entered the **auto qos classify** command, the switch automatically creates class maps and policy maps (as shown below).
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY

If you entered the `auto qos classify police` command, the switch automatically creates class maps and policy maps (as shown below).

Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap)# policy 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap)# policy 10000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap)# policy 32000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default

This is the enhanced configuration for the `auto qos voip cisco-phone` command:

Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_VOIP_VIDEO_CLASS
Switch(config-cmap)# match ip dscp af41
Switch(config)# class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
Switch(config)# class-map match-all AUTOQOS_DEFAULT_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-DEFAULT
Switch(config)# policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap)# class AUTOQOS_VOIP_VIDEO_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default

Switch(config-if)# service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY

This is the enhanced configuration for the auto qos voip cisco-softphone command:

Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_TRANSACTION_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
Switch(config)# class-map match-all AUTOQOS_SCAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# class-map match-all AUTOQOS_SIGNALING_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SIGNALING

Switch(config)# policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap)# police 5000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_BULK_DATA_CLASS
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap)# class AUTOQOS_TRANSACTION_CLASS
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap)# class AUTOQOS_SCAVANGER_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap)# police 1000000 8000 exceed-action drop
Switch(config-pmap)# class AUTOQOS_SIGNALING_CLASS
Switch(config-pmap-c)# set dscp default
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY

auto qos global compact

The following is an example of the auto qos global compact command.

Switch# configure terminal
Switch(config)# auto qos global compact
Switch(config)# interface GigabitEthernet0/2
Switch(config-if)# auto qos voip cisco-phone

Switch# show auto-qos
Switch# show running-config interface GigabitEthernet0/2

interface GigabitEthernet0/2
auto qos voip cisco-phone
end

Where to Go Next for Auto-QoS

Review the QoS documentation if you require any specific QoS changes to your auto-QoS configuration.

Additional References for Auto-QoS

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>Cisco IOS Quality of Service Solutions 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. 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-QoS

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 15.2(6)Ex</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART VII

Routing

• Configuring IP Unicast Routing, on page 457
CHAPTER 25

Configuring IP Unicast Routing

- Finding Feature Information, on page 457
- Information About Configuring IP Unicast Routing, on page 457
- Information About IP Routing, on page 458
- Configuring IP Unicast Routing, on page 460
- Enabling IP Unicast Routing, on page 461
- Assigning IP Addresses to SVIs, on page 462
- Configuring Static Unicast Routes, on page 464
- Configuring Default Routes and Networks, on page 465
- How to Configure RIP, on page 466
- Example: Configuring Summary Addresses and Split Horizon, on page 472
- Example: Displaying Current Status of Routing Table, on page 472
- Monitoring and Maintaining the IP Network, on page 473

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 IP Unicast Routing

This module describes how to configure IP Version 4 (IPv4) unicast routing on the switch.

Note

In addition to IPv4 traffic, you can also enable IP Version 6 (IPv6) unicast routing and configure interfaces to forward IPv6 traffic.
Information About IP Routing

In some network environments, VLANs are associated with individual networks or subnetworks. In an IP network, each subnetwork is mapped to an individual VLAN. Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, network devices in different VLANs cannot communicate with one another without a Layer 3 device (router) to route traffic between the VLAN, referred to as inter-VLAN routing. You configure one or more routers to route traffic to the appropriate destination VLAN.

Figure 46: Routing Topology Example

This figure shows a basic routing topology. Switch A is in VLAN 10, and Switch B is in VLAN 20. The router has an interface in each VLAN.

When Host A in VLAN 10 needs to communicate with Host B in VLAN 10, it sends a packet addressed to that host. Switch A forwards the packet directly to Host B, without sending it to the router.

When Host A sends a packet to Host C in VLAN 20, Switch A forwards the packet to the router, which receives the traffic on the VLAN 10 interface. The router checks the routing table, finds the correct outgoing interface, and forwards the packet on the VLAN 20 interface to Switch B. Switch B receives the packet and forwards it to Host C.

Types of Routing

Routers and Layer 3 switches can route packets in these ways:

- By using default routing
- By using preprogrammed static routes for the traffic
- By dynamically calculating routes by using a routing protocol

The switch supports static routes and default routes. It does not support routing protocols.

The switch supports static routes and default routes. It supports Routing Information Protocol (RIP) for both IPv4 and IPv6 versions.

Static Unicast Routes

Static unicast routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the router cannot build a route to a particular destination and are useful for specifying a gateway of last resort to which all unroutable packets are sent.

The switch retains static routes until you remove them. However, you can override static routes with dynamic routing information by assigning administrative distance values. Each dynamic routing protocol has a default administrative distance, as listed in Table 41-16. If you want a static route to be overridden by information
from a dynamic routing protocol, set the administrative distance of the static route higher than that of the
dynamic protocol.

**Table 60: Dynamic Routing Protocol Default Administrative Distances**

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route</td>
<td>1</td>
</tr>
<tr>
<td>Enhanced IRGP summary route</td>
<td>5</td>
</tr>
<tr>
<td>Internal Enhanced IGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>Unknown</td>
<td>225</td>
</tr>
</tbody>
</table>

Static routes that point to an interface are advertised through RIP, IGRP, and other dynamic routing protocols,
whether or not static `redistribute` router configuration commands were specified for those routing protocols.
These static routes are advertised because static routes that point to an interface are considered in the routing
table to be connected and hence lose their static nature. However, if you define a static route to an interface
that is not one of the networks defined in a network command, no dynamic routing protocols advertise the
route unless a `redistribute` static command is specified for these protocols.

When an interface goes down, all static routes through that interface are removed from the IP routing table.
When the software can no longer find a valid next hop for the address specified as the forwarding router's
address in a static route, the static route is also removed from the IP routing table.

**Default Routes and Networks**

A router might not be able to learn the routes to all other networks. To provide complete routing capability,
you can use some routers as smart routers and give the remaining routers default routes to the smart router.
(Smart routers have routing table information for the entire internetwork.) These default routes can be
dynamically learned or can be configured in the individual routers. Most dynamic interior routing protocols
include a mechanism for causing a smart router to generate dynamic default information that is then forwarded
to other routers.

If a router has a directly connected interface to the specified default network, the dynamic routing protocols
running on that device generate a default route. In RIP, it advertises the pseudonetwork 0.0.0.0.

A router that is generating the default for a network also might need a default of its own. One way a router
can generate its own default is to specify a static route to the network 0.0.0.0 through the appropriate device.

When default information is passed through a dynamic routing protocol, no further configuration is required.
The system periodically scans its routing table to choose the optimal default network as its default route. In
IGRP networks, there might be several candidate networks for the system default. Cisco routers use
administrative distance and metric information to set the default route or the gateway of last resort.
If dynamic default information is not being passed to the system, candidates for the default route are specified with the `ip default-network` global configuration command. If this network appears in the routing table from any source, it is flagged as a possible choice for the default route. If the router has no interface on the default network, but does have a path to it, the network is considered as a possible candidate, and the gateway to the best default path becomes the gateway of last resort.

**Routing Information Protocol**

The Routing Information Protocol (RIP) is an interior gateway protocol (IGP) created for use in small, homogeneous networks. It is a distance-vector routing protocol that uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The protocol is documented in RFC 1058. You can find detailed information about RIP in *IP Routing Fundamentals*, published by Cisco Press.

Using RIP, the Switch sends routing information updates (advertisements) every 30 seconds. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by that router as unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the non-updating router.

RIP uses hop counts to rate the value of different routes. The hop count is the number of routers that can be traversed in a route. A directly connected network has a hop count of zero; a network with a hop count of 16 is unreachable. This small range (0 to 15) makes RIP unsuitable for large networks.

If the router has a default network path, RIP advertises a route that links the router to the pseudonetwork 0.0.0.0. The 0.0.0.0 network does not exist; it is treated by RIP as a network to implement the default routing feature. The Switch advertises the default network if a default was learned by RIP or if the router has a gateway of last resort and RIP is configured with a default metric. RIP sends updates to the interfaces in specified networks. If an interface’s network is not specified, it is not advertised in any RIP update.

**Summary Addresses and Split Horizon**

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature usually optimizes communication among multiple routers, especially when links are broken.

**Configuring IP Unicast Routing**

By default, IP routing is disabled on the switch. For detailed IP routing configuration information, see the *Cisco IOS IP Configuration Guide, Release 12.2* from the *Cisco.com* page under Documentation > Cisco IOS Software Releases > 12.2 Mainline > Configuration Guides.

In these procedures, the specified interface can be a switch virtual interface (SVI)-a VLAN interface or a physical port interface created by using the `interface vlan vlan_id` or `interface type number` global configuration commands respectively, and by default a Layer 3 interface. All Layer 3 interfaces on which routing will occur must have IP addresses assigned to them.

**Note**

The switch supports 16 static routes (including user-configured routes and the default route) and any directly connected routes and default routes for the management interface.
Procedures for configuring routing:

- To support VLAN interfaces, create and configure VLANs on the switch, and assign VLAN membership to Layer 2 interfaces. For more information, see chapter: Configuring VLANs.
- Configure Layer 3 interfaces.
- Enable IP routing on the switch.
- Assign IP addresses to the Layer 3 interfaces.
- Configure static routes.

## Enabling IP Unicast Routing

By default, the Switch is in Layer 2 switching mode and IP routing is disabled. To use the Layer 3 capabilities of the Switch, you must enable IP routing.

### Procedure

<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></td>
<td>Switch&gt; enable</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>ip routing</td>
<td>Enables IP routing.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch(config)# ip routing</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch# show running-config</td>
</tr>
</tbody>
</table>
Example: Enabling IP Unicast Routing

This example shows how to enable IP unicast routing.

```
Device(config)# ip routing
Device(config)# end
Device# show running-config
Device# copy running-config startup-config
```

Assigning IP Addresses to SVIs

To configure IP routing, you need to assign IP addresses to Layer 3 network interfaces. This enables communication with the hosts of those interfaces that use IP. IP routing is disabled by default, and no IP addresses are assigned to SVIs.

An IP address identifies a location to which IP packets can be sent. Some IP addresses are reserved for special uses and cannot be used for host, subnet, or network addresses. RFC 1166, “Internet Numbers,” contains the official description of IP addresses.

An interface can have one primary IP address. A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is referred to as a subnet mask. To receive an assigned network number, contact your Internet service provider.

Follow these steps to assign an IP address and a network mask to an SVI:

### 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><code>enable</code></td>
<td>Enables privileged EXEC mode.</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><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
Step 3 | Enters interface configuration mode, and specifies the Layer 3 VLAN to configure.

**Step 4**  
**ip address ip-address subnet-mask**  
*Example:*  
Switch(config-if)# ip address 10.1.5.1 255.255.255.0

**Step 5**  
**end**  
*Example:*  
Switch(config)# end

**Step 6**  
**show interfaces vlan [vlan-id]**  
*Example:*  
Switch# show interfaces vlan 4

**Step 7**  
**show running-config**  
*Example:*  
Switch# show running-config

**Step 8**  
**copy running-config startup-config**  
(Optional) Saves your entries in the configuration file.

**Example: Assigning IP Addresses to SVIs**

This example shows how to assign an IP address and a network mask to an SVI.

```
Device(config)# interface vlan 4  
Device(config-if)# ip address 10.1.5.1 255.255.255.0  
Device(config-if)# exit  
Device# show interfaces vlan 4  
Device# show running-config  
Device# copy running-config startup-config
```
Configuring Static Unicast Routes

Static unicast routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the router cannot build a route to a particular destination and are useful for specifying a gateway of last resort to which all unroutable packets are sent.

**Note**

Static routing is supported on Catalyst 2960-L switches from Cisco IOS Release 15.2(5)E2 and higher.

Follow these steps to configure a static route:

**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>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>ip route prefix mask {address</td>
<td>interface} [distance]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip route prefix mask gigabitethernet 0/4</td>
<td></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 route</td>
<td>Displays the current state of the routing table to verify the configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip route</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>
</tbody>
</table>
### Example: Configuring Static Unicast Routes

This example shows how to configure static unicast routes.

```
Device(config)# ip route prefix mask gigabitethernet 0/4
Device(config)# end
Device(config)# show ip route
Device(config)# copy running-config startup-config
```

### Configuring Default Routes and Networks

#### 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>ip route network number</td>
<td>Specifies a default network.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2</td>
<td></td>
</tr>
<tr>
<td>3</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>4</td>
<td>show ip route</td>
<td>Displays the selected default route in the gateway of last resort display.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show ip route</td>
<td></td>
</tr>
<tr>
<td>5</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>
</tbody>
</table>
Switch# copy running-config startup-config

How to Configure RIP

Default RIP Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto summary</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Default-information originate</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Default metric</td>
<td>Built-in; automatic metric translations.</td>
</tr>
<tr>
<td>IP RIP authentication key-chain</td>
<td>No authentication. Authentication mode: clear text.</td>
</tr>
<tr>
<td>IP RIP triggered</td>
<td>Disabled</td>
</tr>
<tr>
<td>IP split horizon</td>
<td>Varies with media.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>None defined.</td>
</tr>
<tr>
<td>Network</td>
<td>None specified.</td>
</tr>
<tr>
<td>Offset list</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Output delay</td>
<td>0 milliseconds.</td>
</tr>
<tr>
<td>Timers basic</td>
<td>• Update: 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Invalid: 180 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Hold-down: 180 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Flush: 240 seconds.</td>
</tr>
<tr>
<td>Validate-update-source</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Version</td>
<td>Receives RIP Version 1 and 2 packets; sends Version 1 packets.</td>
</tr>
</tbody>
</table>
# Configuring Basic RIP Parameters

To configure RIP, you enable RIP routing for a network and optionally configure other parameters. On the Switch, RIP configuration commands are ignored until you configure the network number.

## Procedure

<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 | ip routing | Enables IP routing. (Required only if IP routing is disabled.)  
**Example:**

Switch(config) # ip routing |
| Step 4 | router rip | Enables a RIP routing process, and enter router configuration mode.  
**Example:**

Switch(config) # router rip |
| Step 5 | network network number | Associates a network with a RIP routing process. You can specify multiple network commands. RIP routing updates are sent and received through interfaces only on these networks.  
**Note:** You must configure a network number for the RIP commands to take effect.  
**Example:**

Switch(config-router) # network 12.0.0.0 |
| Step 6 | neighbor ip-address | (Optional) Defines a neighboring router with which to exchange routing information. This step allows routing updates from RIP (normally a broadcast protocol) to reach nonbroadcast networks.  
**Example:**

Switch(config-router) # neighbor 10.2.5.1 |
| Step 7 | offset-list [access-list number | name] [in | out] offset [type number] | (Optional) Applies an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through RIP. You can limit the offset list with an access list or an interface.  
**Example:**

Switch(config-router) # offset-list 103 in 10 |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> timers basic update invalid holddown flush</td>
<td>(Optional) Adjusts routing protocol timers. Valid ranges for all timers are 0 to 4294967295 seconds.</td>
</tr>
<tr>
<td>Example: Switch(config-router)# timers basic 45 360 400 300</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> version {1 | 2}</td>
<td>(Optional) Configures the switch to receive and send only RIP Version 1 or RIP Version 2 packets. By default, the switch receives Version 1 and 2 but sends only Version 1. You can also use the interface commands <strong>ip rip</strong> {send | receive} <strong>version</strong> {1 | 2} to control what versions are used for sending and receiving on interfaces.</td>
</tr>
<tr>
<td>Example: Switch(config-router)# version 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> no auto summary</td>
<td>(Optional) Disables automatic summarization. By default, the switch summarizes subprefixes when crossing classful network boundaries. Disable summarization (RIP Version 2 only) to advertise subnet and host routing information to classful network boundaries.</td>
</tr>
<tr>
<td>Example: Switch(config-router)# no auto summary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config-router)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> show ip protocols</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example: Switch# show ip protocols</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</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>

**Configuring RIP Authentication**

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface. The key chain specifies the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed, not even the default.
The Switch supports two modes of authentication on interfaces for which RIP authentication is enabled: plain text and MD5. The default is plain text.

### Procedure

<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>
</tbody>
</table>
| enable            | Enables privileged EXEC mode.  
| Example:          | • Enter your password if prompted. |
| Switch> enable    |                     |

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

| **Step 3**        | **Purpose** |
| interface interface-id | Enters interface configuration mode, and specifies the interface to configure. |
| Example:          |                     |
| Switch(config)# interface gigabitethernet 0/1 |                     |

| **Step 4**        | **Purpose** |
| ip rip authentication key-chain name-of-chain | Enables RIP authentication. |
| Example:          |                     |
| Switch(config-if)# ip rip authentication key-chain trees |                     |

| **Step 5**        | **Purpose** |
| ip rip authentication mode {text | md5} | Configures the interface to use plain text authentication (the default) or MD5 digest authentication. |
| Example:          |                     |
| Switch(config-if)# ip rip authentication mode md5 |                     |

| **Step 6**        | **Purpose** |
| end               | Returns to privileged EXEC mode. |
| Example:          |                     |
| Switch(config)# end |                     |

| **Step 7**        | **Purpose** |
| show running-config | Verifies your entries. |
| Example:          |                     |
| Switch# show running-config |                     |

| **Step 8**        | **Purpose** |
| copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
| Example:          |                     |
### Configuring Summary Addresses and Split Horizon

#### Purpose

**Command or Action**

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

#### Note

In general, disabling split horizon is not recommended unless you are certain that your application requires it to properly advertise routes.

If you want to configure an interface running RIP to advertise a summarized local IP address pool on a network access server for dial-up clients, use the `ip summary-address rip` interface configuration command.

#### Note

If split horizon is enabled, neither autosummary nor interface IP summary addresses are advertised.

### Procedure

<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>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface <code>interface-id</code></td>
<td>Enters interface configuration mode, and specifies the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address <code>ip-address subnet-mask</code></td>
<td>Configures the IP address and IP subnet.</td>
</tr>
<tr>
<td>Example: <code>Switch(config-if)# ip address 10.1.1.10 255.255.255.0</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <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>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show ip interface interface-id</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show ip interface gigabitethernet 0/1</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:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Split Horizon

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature can optimize communication among multiple routers, especially when links are broken.

**Note**  In general, we do not recommend disabling split horizon unless you are certain that your application requires it to properly advertise routes.

### Procedure

<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>Enters interface configuration mode, and specifies the interface to configure.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>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 4</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>ip address ip-address subnet-mask</td>
<td>Configures the IP address and IP subnet.</td>
</tr>
<tr>
<td>Switch(config-if)# ip address 10.1.1.10 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>show ip interface interface-id</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Switch# show ip interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**Example: Configuring Summary Addresses and Split Horizon**

In this example, the major net is 10.0.0.0. The summary address 10.2.0.0 overrides the autosummary address of 10.0.0.0 so that 10.2.0.0 is advertised out interface Gigabit Ethernet port 2, and 10.0.0.0 is not advertised. In the example, if the interface is still in Layer 2 mode (the default), you must enter a no switchport interface configuration command before entering the ip address interface configuration command.

**Note**

If split horizon is enabled, neither autosummary nor interface summary addresses (those configured with the ip summary-address rip router configuration command) are advertised.

Switch(config)# router rip
Switch(config-router)# interface gigabitethernet0/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end

**Example: Displaying Current Status of Routing Table**

This is an example of the output from the show ip route privileged EXEC command:
Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.0.2.5 to network 0.0.0.0

S* 0.0.0.0/0 [0/0] via 192.0.2.5
3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 3.3.3.0/24 is directly connected, GigabitEthernet0/23
L 3.3.3.2/32 is directly connected, GigabitEthernet0/23
6.0.0.0/24 is subnetted, 1 subnets
S 6.6.6.0 [1/0] via 192.0.2.5
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 192.0.2.4/24 is directly connected, Vlan1
L 192.0.2.10/24 is directly connected, Vlan1
40.0.0.0/24 is subnetted, 1 subnets
S 40.40.40.0 [1/0] via 192.0.2.5
Device#

S -- Stand for static route.

## Monitoring and Maintaining the IP Network

You can remove all contents of a particular cache, table, or database. You can also display specific statistics.

### Table 62: Commands to Clear IP Routes or Display Route Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip route [address [mask] [longer-prefixes]]</td>
<td>Displays the current state of the routing table.</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Displays the current state of the routing table in summary form.</td>
</tr>
</tbody>
</table>
PART VIII

Security

- Security Features Overview, on page 477
- Preventing Unauthorized Access, on page 481
- Controlling Switch Access with Passwords and Privilege Levels, on page 483
- Configuring TACACS+, on page 499
- 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 625
- AAA-SERVER-MIB Set Operation, on page 633
- Configuring Secure Shell, on page 639
- Secure Shell Version 2 Support, on page 657
- X.509v3 Certificates for SSH Authentication, on page 681
- Configuring Secure Socket Layer HTTP, on page 695
- Certification Authority Interoperability, on page 709
- Access Control List Overview, on page 725
- Configuring IPv4 Access Control Lists, on page 735
- IPv6 Access Control Lists, on page 771
- Configuring DHCP, on page 787
- Configuring IP Source Guard, on page 811
- Configuring IEEE 802.1x Port-Based Authentication, on page 819
- Configuring IPv6 First Hop Security, on page 889
- Per-User ACL Support for 802.1X/MAB/Webauth Users, on page 921
- Web Authentication Redirection to Original URL, on page 927
• Configuring Web-Based Authentication, on page 931
• Configuring Port-Based Traffic Control, on page 961
Security Features Overview

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.

• IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. The following 802.1x features are supported:
  • Support for single-host, multi-host, multi-auth, and multi-domain-auth modes.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-Host</td>
<td>Only one host can be authenticated. Security violation occurs if more than one client tries to authenticate.</td>
</tr>
<tr>
<td>Multi-Host</td>
<td>Only first host needs to authenticate. Remaining hosts get access without authentication.</td>
</tr>
<tr>
<td>Multi-Auth</td>
<td>Every client must get authenticated.</td>
</tr>
<tr>
<td>Multi-Domain-Auth</td>
<td>One VoIP client and one data client is allowed to authenticate. Security violation occurs if more than one client tries to authenticate.</td>
</tr>
</tbody>
</table>

• 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.

• 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 with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame.

• 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.

• 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.

• IEEE 802.1x with open access to allow a host to access the network before being authenticated.

• IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a RADIUS server or Cisco Identity Services Engine (ISE) to an authenticated switch.

• Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs.

• Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.

• 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.

• Enhancements to RADIUS, TACACS+, and SSH functionality.

• 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.

• 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.

• 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.

• 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.
• MAC address based authentication using MAC Authentication Bypass (MAB). Authenticated hosts are moved to a dynamic VLAN 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.

• Cisco TrustSec SXP protocol is not supported.

Feature Information for Security Features

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(6)E2</td>
<td>The following features were introduced:</td>
</tr>
<tr>
<td></td>
<td>• IEEE 802.1x authentication with downloadable ACLs and redirect URLs.</td>
</tr>
<tr>
<td></td>
<td>• Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs.</td>
</tr>
<tr>
<td></td>
<td>• IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute.</td>
</tr>
<tr>
<td></td>
<td>• Support for IP source guard on static hosts.</td>
</tr>
<tr>
<td></td>
<td>• IEEE 802.1x User Distribution to allow deployments with multiple VLANs</td>
</tr>
</tbody>
</table>
Preventing Unauthorized Access

• Finding Feature Information, on page 481
• Preventing Unauthorized Access, on page 481

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.
CHAPTER 28

Controlling Switch Access with Passwords and Privilege Levels

- Finding Feature Information, on page 483
- Restrictions for Controlling Switch Access with Passwords and Privileges, on page 483
- Information About Passwords and Privilege Levels, on page 484
- How to Control Switch Access with Passwords and Privilege Levels, on page 486
- Monitoring Switch Access, on page 496
- Configuration Examples for Setting Passwords and Privilege Levels, on page 497
- Additional References, on page 497

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.
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.

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.

**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.

**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.

**Privilege Levels**

Cisco 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.
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 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><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> enable password password</td>
<td>Defines a new password or changes an existing password for access to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# enable password secret321</td>
<td>By default, no password is defined.</td>
</tr>
<tr>
<td></td>
<td>For <em>password</em>, 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. It can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password abc?123, do this:</td>
</tr>
<tr>
<td></td>
<td>a. Enter <strong>abc</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Enter <strong>Ctrl-v</strong>.</td>
</tr>
</tbody>
</table>
Purpose

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abe?123 at the password prompt.

Step 4

<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

Step 5

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>

Example:

Switch# show running-config

Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Example:

Switch# copy running-config startup-config

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
<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 | Use one of the following: 
  - `enable password [level level] {password encryption-type encrypted-password}` 
  - `enable secret [level level] {password encryption-type encrypted-password}` | 
  Example: 
  Switch(config)# enable password example102  
  or  
  Switch(config)# enable secret level 1 password secret123sample |
| Step 4 | 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. 
  Example: 
  Switch(config)# service password-encryption |

**Note** 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.
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>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>
</tbody>
</table>
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

---

### Command or Action | Purpose
---

**Step 2**

Configure terminal

*Example:*

Switch# configure terminal

**Step 3**

System disable password recovery switch <1-9>

*Example:*

Switch(config)# system disable password recovery switch all

Disables password recovery.

- *all* - Sets the configuration on switches in stack.
- *<1-9>* - Sets the configuration on the Switch Number selected.

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**

End

*Example:*

Switch(config)# end

Returns to privileged EXEC mode.

---

**What to do next**

To remove disable password recovery, use the no system disable password recovery switch all global configuration command.

---

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
<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><strong>Note</strong> 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>Example:</td>
<td><code>Switch&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>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>line vty 0 15</code></td>
<td>Configures the number of Telnet sessions (lines), and enters line configuration mode. 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>
<tr>
<td>Example:</td>
<td><code>Switch(config)# line vty 0 15</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>password password</code></td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch(config-line)# password abcxyz543</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>Example:</td>
<td><code>Switch(config-line)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<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><code>Switch# copy running-config startup-config</code></td>
<td></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
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>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> username name [privilege level] {password encryption-type password}</td>
<td>Sets the username, privilege level, and password for each user.</td>
</tr>
<tr>
<td>Example: Switch(config)# username adamsample privilege 1 password secret456</td>
<td>• For name, specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed.</td>
</tr>
<tr>
<td></td>
<td>• You can configure a maximum of 12000 clients each, for both username and MAC filter.</td>
</tr>
<tr>
<td></td>
<td>• (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.</td>
</tr>
<tr>
<td></td>
<td>• For encryption-type, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow.</td>
</tr>
<tr>
<td></td>
<td>• 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.</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>Use one of the following:</td>
</tr>
<tr>
<td>• line console 0</td>
<td>Enters line configuration mode, and configures the console port (line 0) or the VTY lines (line 0 to 15).</td>
</tr>
<tr>
<td>• line vty 0 15</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# line console 0</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# line vty 15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>login local</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables local password checking at login time. Authentication is based on the username specified in Step 3.</td>
</tr>
<tr>
<td>Switch(config-line)# login local</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

**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> 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# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> privilege mode level level command</td>
<td>Sets the privilege level for a command.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# privilege exec level 14 configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enable password level level password</td>
<td>Specifies the password to enable the privilege level.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# enable password level 14 SecretPswd14</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> 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>
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>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>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>line vty line</code></td>
<td>Selects the virtual terminal line on which to restrict access.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# line vty 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>privilege level level</code></td>
<td>Changes the default privilege level for the line.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# privilege level 15</code></td>
<td>For <code>level</code>, 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 <code>enable</code> password.</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <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>
</tbody>
</table>
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.

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> <code>enable level</code></td>
<td>Logs in to a specified privilege level. Following the example, Level 15 is privileged EXEC mode. For <code>level</code>, the range is 0 to 15.</td>
</tr>
<tr>
<td>Example: <code>Switch&gt; enable 15</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>disable level</code></td>
<td>Exits to a specified privilege level. Following the example, Level 1 is user EXEC mode. For <code>level</code>, the range is 0 to 15.</td>
</tr>
<tr>
<td>Example: <code>Switch# disable 1</code></td>
<td></td>
</tr>
</tbody>
</table>

Monitoring Switch Access

**Table 64: Commands for Displaying DHCP Information**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show privilege</code></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
```

Example: Protecting Enable and Enable Secret Passwords with Encryption

This example shows how to configure the encrypted password $1$FaD0$Xyti5Rkls3LoyxzS8 for privilege level 2:

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

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
```

Example: Setting the Privilege Level for a Command

This example shows how to set the configure command to privilege level 14 and define SecretPswwd14 as the password users must enter to use level 14 commands:

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswwd14
```

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></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:</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>
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 499
- Prerequisites for TACACS+, on page 499
- Restrictions for TACACS+, on page 500
- Information About TACACS+, on page 500
- How to Configure TACACS+, on page 523
- Configuration Examples for TACACS+, on page 533
- Additional References for TACACS+, on page 537
- Feature Information for TACACS+, on page 538

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.
- 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.
**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—independently. 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 47: 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 audit or
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:
   - Telnet, Secure Shell (SSH), rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and user timeouts

**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.

If a method list is configured under VTY lines, the corresponding method list must be added to AAA. The
following example shows how to configure a method list under a VTY line:

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

The following example shows how to configure a method list in AAA:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```

If no method list is configured under VTY lines, the default method list must be added to AAA. The following
example shows a VTY configuration without a method list:

```
Device# configure terminal
Device(config)# line vty 0 4
```

The following example shows how to configure the default method list:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+
```

**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>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>
</tbody>
</table>
| addr-pool=x   | Specifies the name of a local pool from which to get the address of the remote host. Used with service=ppp and protocol=ip. 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: ip address-pool local
ip local pool boo 10.0.0.1 10.0.0.10
ip local pool moo 10.0.0.1 10.0.0.20
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. | yes  | yes  | yes  | yes  | yes  | yes  | yes  |
| autocmd=x     | Specifies an autocommand to be executed at EXEC startup (for example, autocmd=telnet example.com). Used only with service=shell. | yes  | yes  | yes  | yes  | yes  | yes  | yes  |
| callback- dialstring | 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. | no   | yes  | yes  | yes  | yes  | yes  | yes  |
| callback-line | 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. | no   | yes  | yes  | yes  | yes  | yes  | yes  |
| callback-rotary | 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. | no   | yes  | yes  | yes  | yes  | yes  | yes  |
| cmd-arg=x     | 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.  

*Note* This TACACS+ AV pair cannot be used with RADIUS attribute 26. | yes  | yes  | yes  | yes  | yes  | yes  | yes  |
| cmd=x         | 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.  

*Note* This TACACS+ AV pair cannot be used with RADIUS attribute 26. | yes  | yes  | yes  | yes  | yes  | yes  | yes  |
<p>| data-service  | Used with the service=outbound and protocol=ip. | no   | no   | no   | no   | yes  | yes  |</p>
<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>dial-number</td>
<td>Defines the number to dial. Used with service=outbound and protocol=ip.</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td></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>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.</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>Note: This attribute replaces the “interface-config=” attribute.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>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>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>no</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>no</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>no</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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. Link compression is defined as a numeric value as follows:</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></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>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>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>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>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>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>
| port-type          | 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:  
  - 0: Asynchronous  
  - 1: Synchronous  
  - 2: ISDN-Synchronous  
  - 3: ISDN-Asynchronous (V.120)  
  - 4: ISDN-Asynchronous (V.110)  
  - 5: Virtual  
  Used with service=any and protocol=aaa.                                                                                       | no   | no   | no   | no   | no   | yes  | yes  |
<p>| ppp-vj-slot-       | Instructs the Cisco router not to use slot compression when sending VJ-compressed packets over a PPP link.                                                                                          | no   | no   | no   | yes  | yes  | yes  | yes  |
| compression        |                                                                                                                                                                                                            |      |      |      |      |      |      |      |
| priv-lvl=x         | Privilege level to be assigned for the EXEC. Used with service=shell. Privilege levels range from 0 to 15, with 15 being the highest.                                                                  | yes  | yes  | yes  | yes  | yes  | yes  | yes  |
| protocol=x         | 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, cec, cdp, bridging, xns, nbf, bap, multilink, and unknown. | yes  | yes  | yes  | yes  | yes  | yes  | yes  |
| proxyacl#&lt;n&gt;       | 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. | no   | no   | no   | no   | no   | yes  | yes  |</p>
<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</td>
<td>Specifies a route to be applied to an interface. Used with service=slip, service=ppp, and protocol=ip. During network authorization, the route attribute can be used to specify a per-user static route, to be installed by TACACS+ as follows: route=&quot;dst_address mask [gateway]&quot; 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.</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>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>no</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>
</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>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>yes</td>
<td>yes</td>
<td></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>
<tr>
<td>spi</td>
<td>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 &lt;addr&gt; 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.</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>timeout=x</td>
<td>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.</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>tunnel-id</td>
<td>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.</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>wins-servers=x</td>
<td>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.</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>zonelist=x</td>
<td>A numeric zonelist value. Used with service=arap. Specifies an AppleTalk zonelist for ARA (for example, zonelist=5).</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

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 66: Supported 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>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>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>bytes_in</td>
<td>The number of input bytes transferred during this connection.</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>bytes_out</td>
<td>The number of output bytes transferred during this connection.</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>Call-Type</td>
<td>Describes the type of fax activity: fax receive or fax send.</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>cmd</td>
<td>The command the user executed.</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-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>no</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>no</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>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>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>no</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>no</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>no</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</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>yes</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>yes</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>yes</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>no</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
## TACACS Accounting AV Pairs

### Attribute | Description | 11.0 | 11.1 | 11.2 | 11.3 | 12.0 | 12.1 | 12.2
---|---|---|---|---|---|---|---|---
pre-bytes-in | Records the number of input bytes before authentication. This attribute is sent in accounting-stop records. | no | no | no | yes | yes | yes | yes
pre-bytes-out | Records the number of output bytes before authentication. This attribute is sent in accounting-stop records. | no | no | no | yes | yes | yes | yes
pre-paks-in | Records the number of input packets before authentication. This attribute is sent in accounting-stop records. | no | no | no | yes | yes | yes | yes
pre-paks-out | Records the number of output packets before authentication. The Pre-Output-Packets attribute is sent in accounting-stop records. | no | no | no | yes | yes | yes | yes
pre-session-time | Specifies the length of time, in seconds, from when a call first connects to when it completes authentication. | no | no | no | yes | yes | yes | yes
priv_level | The privilege level associated with the action. | yes | yes | yes | yes | yes | yes | yes
protocol | The protocol associated with the action. | yes | yes | yes | yes | yes | yes | yes
reason | 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). | yes | yes | yes | yes | yes | yes | yes
service | The service the user used. | yes | yes | yes | yes | yes | yes | yes
start_time | 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. | yes | yes | yes | yes | yes | yes | yes
stop_time | The time the action stopped (in seconds since the epoch.) The clock must be configured to receive this information. | yes | yes | yes | yes | yes | yes | yes
task_id | Start and stop records for the same event must have matching (unique) task_id numbers. | yes | yes | yes | yes | yes | yes | yes
timezone | The time zone abbreviation for all timestamps included in this packet. | yes | yes | yes | yes | yes | yes | yes
xmit-rate | This AV pair has been renamed. See nas-tx-speed. | yes | yes | yes | yes | yes | yes | yes

The following table lists the cause codes and descriptions for the Disconnect Cause Extended (disc-cause-ext) attribute.

### Table 67: Disconnect Cause Extensions

| Cause Codes | Description | 11.0 | 11.1 | 11.2 | 11.3 | 12.0 | 12.1 | 12.2 | 12.3 |
---|---|---|---|---|---|---|---|---|---|
1000 - No Reason | No reason for the disconnect. | no | no | no | no | yes | yes | yes | yes |
1001 - No Disconnect | The event was not a disconnect. | no | no | no | no | yes | yes | yes | yes |
1002 - Unknown | The reason for the disconnect is unknown. This code can appear when the remote connection goes down. | no | no | no | no | yes | yes | yes | yes |
<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>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>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>no</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>no</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>no</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>no</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>no</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>no</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>no</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>no</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>no</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>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>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>no</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>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</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>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>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>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</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>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>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></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></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></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></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></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></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></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></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></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></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></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></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></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></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></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></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></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></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>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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>no</td>
<td>yes</td>
<td>yes</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>yes</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>yes</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>yes</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>yes</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>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>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>no</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>yes</td>
<td>no</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>yes</td>
<td>no</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>yes</td>
<td>no</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>yes</td>
<td>no</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>yes</td>
<td>no</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>yes</td>
<td>no</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>yes</td>
<td>no</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>yes</td>
<td>no</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>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>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>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>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>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. 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 | Description | 11.0 | 11.1 | 11.2 | 11.3 | 12.0 | 12.1 | 12.2 | 12.3
--- | --- | --- | --- | --- | --- | --- | --- | --- | ---
1900 - Q850 Invalid Element Contents | 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. | no | no | no | no | no | no | no | yes
1901 - Q850 Wrong Message for State | 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. | no | no | no | no | no | no | no | yes
1902 - Q850 Recovery on Timer Expiration | 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. | no | no | no | no | no | no | no | yes
1903 - Q850 Info Element Error | 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. | no | no | no | no | no | no | no | yes
1911 - Q850 Protocol Error | 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. | no | no | no | no | no | no | no | yes
1927 - Q850 Unspecified Internetworking Event | 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. | no | no | no | no | no | no | no | yes

**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.

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.

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. aaa new-model
4. aaa group server tacacs+ group-name
5. server ip-address
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>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> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa group server tacacs+ group-name</td>
<td>(Optional) Defines the AAA server-group with a group name.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa group server tacacs+ your_server_group</td>
<td>This command puts the Switch in a server group subconfiguration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> server ip-address</td>
<td>(Optional) Associates a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group.</td>
</tr>
<tr>
<td>Example: Switch(config)# server 10.1.2.3</td>
<td>Each server in the group must be previously defined in Step 3.</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>
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} method [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></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>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**        |         |
| `aaa new-model`   | Enables AAA. |
| Example:          |         |
| Switch(config)# `aaa new-model` | |

<p>| <strong>Step 4</strong>        | Creates a login authentication method list. |
| <code>aaa authentication login {default | list-name} method1 [method2...]</code> | • To create a default list that is used when a named list is not specified in the <code>login authentication</code> command, use the <code>default</code> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports. |
| Example:          | • For <code>list-name</code>, specify a character string to name the list you are creating. |
| Switch(config)# <code>aaa authentication login default tacacs+ local</code> | • For <code>method1...</code>, 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: |
|                   | • <code>enable</code>—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the <code>enable password</code> global configuration command. |
|                   | • <code>group tacacs+</code>—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. |
|                   | • <code>line</code>—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the <code>password password</code> line configuration command. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• local—Use the local username database for authentication. You must enter username information in the database. Use the <code>username password</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• local-case—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the <code>username name password</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• none—Do not use any authentication for login.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

```bash
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**

```bash
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**

```bash
end
```

Example:

```
Switch(config-line)# end
```

Returns to privileged EXEC mode.

**Step 8**

```bash
show running-config
```

Example:

```
Switch# show running-config
```

Verifies your entries.

**Step 9**

```bash
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>
<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><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>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>aaa authorization network tacacs+</code></td>
<td>Configures the switch for user TACACS+ authorization for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization network tacacs+</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>aaa authorization exec tacacs+</code></td>
<td>Configures the switch for user TACACS+ authorization if the user has privileged EXEC access.</td>
</tr>
<tr>
<td>Example:</td>
<td>The <code>exec</code> keyword might return user profile information (such as <code>autocommand</code> information).</td>
</tr>
<tr>
<td><code>Switch(config)# aaa authorization exec tacacs+</code></td>
<td></td>
</tr>
</tbody>
</table>
## 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> 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>
</tbody>
</table>

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

---
### Establishing a Session with a Router if the AAA Server is Unreachable

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.

#### 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.

#### 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Enables TACACS+ accounting for all network-related service requests.</td>
</tr>
<tr>
<td>aaa accounting network start-stop tacacs+</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa accounting network start-stop tacacs+</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables TACACS+ 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>aaa accounting exec start-stop tacacs+</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa accounting exec start-stop tacacs+</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></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>Verifies your entries.</td>
</tr>
<tr>
<td>show running-config</td>
<td></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>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
enable  
**Example:**  
Device> enable  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2**  
**Example:**  
Device# configure terminal  

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Example:**  
Device# configure terminal | Enables privileged EXEC mode.  
- Enter your password if prompted.  

Enters global configuration mode.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> ip vrf vrf-name</td>
<td>Configures a VRF table and enters VRF configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# ip vrf cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> rd route-distinguisher</td>
<td>Creates routing and forwarding tables for a VRF instance.</td>
</tr>
<tr>
<td>Example: Device(config-vrf)# rd 100:1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits VRF configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-vrf)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> interface interface-name</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# interface Loopback0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ip vrf forwarding vrf-name</td>
<td>Configures a VRF for the interface.</td>
</tr>
<tr>
<td>Example: Device(config-if)# ip vrf forwarding cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> ip address ip-address mask [secondary]</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>Example: Device(config-if)# ip address 10.0.0.2 255.0.0.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Exits interface configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> aaa group server tacacs+ group-name</td>
<td>Groups different TACACS+ server hosts into distinct lists and distinct methods and enters server-group configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config)# aaa group server tacacs+ tacacs1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> server-private {ip-address</td>
<td>name} [nat] [single-connection] [port port-number] [timeout seconds] [key [0</td>
</tr>
<tr>
<td>Example: Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco</td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring TACACS+

**Table 68: 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+:

```bash
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:
aaa new-model
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
  ppp authentication chap pap test

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 examples show how to configure TACACS+ as the security protocol for PPP authentication, but instead of the “test” method list, the “default” method list is used.

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”:

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
```

**Example: Configuring Per VRF for TACACS Servers**

The following output example shows that the group server **tacacs1** is configured for per VRF AAA services:
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>MIB Link</th>
<th>MIBs Link</th>
</tr>
</thead>
</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 for TACACS+

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 30

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 579

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 validate 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 48: 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 49: VSA Encapsulated Behind Attribute 26**

![Packet Format](image)

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Vendor-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

---

**Note**

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 69: 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 70: 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></td>
<td></td>
</tr>
</tbody>
</table>

| 26     | 311                          | 1               | MSCHAP-Response | 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. (RFC 2548) |

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
## 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>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>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>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>12tp-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>12tp-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>12tp-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 fix-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>
<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>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></td>
<td></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>
<tr>
<td></td>
<td>H323 Attributes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>23</td>
<td>Remote-Gateway-ID</td>
<td>Indicates the IP address of the remote gateway.</td>
</tr>
<tr>
<td></td>
<td>(h323-remote-address)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>24</td>
<td>Connection-ID</td>
<td>Identifies the conference ID.</td>
</tr>
<tr>
<td></td>
<td>(h323-conf-id)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>25</td>
<td>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></td>
<td>(h323-setup-time)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>26</td>
<td>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></td>
<td>(h323-call-origin)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>27</td>
<td>Call-Type</td>
<td>Indicates call leg type. Possible values are telephony and VoIP.</td>
</tr>
<tr>
<td></td>
<td>(h323-call-type)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>9</td>
<td>28</td>
<td>Connect-Time</td>
<td>Indicates the connection time for this call leg in UTC.</td>
</tr>
<tr>
<td></td>
<td>(h323-connect-time)</td>
<td></td>
<td></td>
<td></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 sent-name password</code> command on the interface. For PAP, &quot;preauth:send-name&quot; and &quot;preauth:send-secret&quot; will be used as the PAP username and PAP password for outbound authentication. For CHAP, &quot;preauth:send-name&quot; 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 &quot;preauth:send-name&quot; 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>
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.

**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>
<tr>
<td>Cause Code</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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><strong>Codes 21, 100, 101, 102, and 120 apply to all session types.</strong></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>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>
</tbody>
</table>

**Note:** Codes 60 through 67 apply to Telnet or raw TCP sessions.
<table>
<thead>
<tr>
<th>Cause Code</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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). 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. 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. 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. 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. Note: 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. Code is sent when there are active sessions in a tunnel and the tunnel goes down. Note: 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. 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. 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>
<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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>+ Enter your password if prompted.</td>
<td></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
<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

Enters global configuration mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>radius server name</td>
<td></td>
</tr>
</tbody>
</table>

Example:

Switch(config)# radius server ISE

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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td></td>
</tr>
</tbody>
</table>
| address {ipv4 | ipv6} ip address {auth-port port number | acct-port port number} | (Optional) Specifies the RADIUS server parameters. For auth-port port-number, specify the UDP destination port for authentication requests. The default is 1645. The range is 0 to 65536. For acct-port port-number, specify the UDP destination port for authentication requests. The default is 1646.

Example:

Switch(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td></td>
</tr>
</tbody>
</table>
| key string        | (Optional) 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. 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.

Example:

Switch(config-radius-server)# key cisco123

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td></td>
</tr>
</tbody>
</table>
| retransmit value  | (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.

Example:

Switch(config-radius-server)# retransmit 10

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td></td>
</tr>
</tbody>
</table>
| timeout seconds   | (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.

Example:

Switch(config-radius-server)# timeout 60
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> 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>

| **Step 2** radius-server key string    | Specifies the shared secret text string used between the switch and all RADIUS servers. |
| Example:                               |                                                                         |
| Switch# radius-server key string       |                                                                         |
Configuring RADIUS Login Authentication

Follow these steps to configure RADIUS login authentication:

**Step 1**

```
Switch(config)# radius-server key your_server_key
```

**Step 2**

```
Switch(config)# key your_server_key
```

**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.

**Step 3**

```
Step 3 radius-server retransmit retries
Example:
Switch(config)# radius-server retransmit 5
```

**Step 4**

```
Step 4 radius-server timeout seconds
Example:
Switch(config)# radius-server timeout 3
```

**Step 5**

```
Step 5 radius-server deadtime minutes
Example:
Switch(config)# radius-server deadtime 0
```

**Step 6**

```
Step 6 end
Example:
Switch(config)# end
```

**Step 7**

```
Step 7 show running-config
Example:
Switch# show running-config
```

**Step 8**

```
Step 8 copy running-config startup-config
Example:
Switch# copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

**Configuring RADIUS Login Authentication**

Follow these steps to configure RADIUS login authentication:
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>
<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> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>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></td>
<td>• To create a default list that is used when a named list is <em>not</em> specified in the <code>login authentication</code> command, use the <code>default</code> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.</td>
</tr>
<tr>
<td>Switch(config)# aaa authentication login default local</td>
<td>• For <code>list-name</code>, specify a character string to name the list you are creating.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>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:</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• group radius—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td>• line—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the password line configuration command.</td>
<td></td>
</tr>
<tr>
<td>• local—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command.</td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
<tr>
<td>• none—Do not use any authentication for login.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

```
line [console | tty | vty] line-number [ending-line-number]
```

Enables line configuration mode, and configure the lines to which you want to apply the authentication list.

**Example:**

```
Switch(config)# line 1 4
```

**Step 6**

```
login authentication {default | list-name}
```

Applies the authentication list to a line or set of lines.

**Example:**

```
Switch(config)# login authentication default
```

**Step 7**

```
end
```

Returns to privileged EXEC mode.

**Example:**
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> <code>enable</code></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> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Purpose |
|------------------|-----------------|
| **Switch# configure terminal** | **Step 3** 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. |
| **radius server name** | **Example:** |
| | Switch(config)# radius server ISE |
| **address {ipv4 | ipv6} {ip-address | hostname} auth-port port-number acct-port port-number** | **Step 4** configures the IPv4 address for the RADIUS server accounting and authentication parameters. |
| **Example:** | Switch(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646 |
| **key string** | **Step 5** specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. |
| **Example:** | Switch(config-radius-server)# key cisco123 |
| **end** | **Step 6** exits RADIUS server configuration mode and returns to privileged EXEC mode. |
| **Example:** | Switch(config-radius-server)# end |
| **show running-config** | **Step 7** verifies your entries. |
| **Example:** | Switch# show running-config |
| **copy running-config startup-config** | **Step 8** (Optional) saves your entries in the configuration file. |
| **Example:** | Switch# copy running-config startup-config |
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>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 aaa authorization network radius</td>
<td>Configures the switch for user RADIUS authorization for all service requests.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa authorization network radius</td>
<td></td>
</tr>
<tr>
<td>Step 4 aaa authorization exec radius</td>
<td>Configures the switch for user RADIUS authorization if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information).</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa authorization exec radius</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

#### Step 5

**Command or Action:**

- `end`

**Example:**

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

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

#### Step 6

**Command or Action:**

- `show running-config`

**Example:**

```
Switch# show running-config
```

**Purpose:** Verifies your entries.

#### Step 7

**Command or Action:**

- `copy running-config startup-config`

**Example:**

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

**Purpose:** (Optional) Saves your entries in the configuration file.

---

**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><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Example</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch&gt; <strong>enable</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 <strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td>Step 3 <strong>aaa accounting network start-stop radius</strong></td>
<td>Enables RADIUS accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <strong>aaa accounting network start-stop radius</strong></td>
<td></td>
</tr>
<tr>
<td>Step 4 <strong>aaa accounting exec start-stop radius</strong></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:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <strong>aaa accounting exec start-stop radius</strong></td>
<td></td>
</tr>
<tr>
<td>Step 5 <strong>end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <strong>end</strong></td>
<td></td>
</tr>
<tr>
<td>Step 6 <strong>show running-config</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# <strong>show running-config</strong></td>
<td></td>
</tr>
<tr>
<td>Step 7 <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# <strong>copy running-config startup-config</strong></td>
<td></td>
</tr>
</tbody>
</table>

### 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.
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> 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> debug aaa accounting</td>
<td>Displays information on accountable events as they occur.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# debug aaa accounting</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show radius statistics</td>
<td>Displays the RADIUS statistics for accounting and authentication packets.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# debug aaa authorization</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 Example: <code>Switch# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 3** radius-server vsa send [accounting | authentication] Example: ```Switch(config)# radius-server vsa send accounting``` | Enables the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26.  
  - (Optional) Use the `accounting` keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.  
  - (Optional) Use the `authentication` keyword to limit the set of recognized vendor-specific attributes to only authentication attributes.  
  If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used. |
| **Step 4** end Example: ```Switch(config)# end``` | Returns to privileged EXEC mode. |
| **Step 5** show running-config Example: ```Switch# show running-config``` | 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. |

### 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></td>
<td><strong>Purpose</strong></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><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>`radius-server host {hostname</td>
<td>ip-address} non-standard`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# radius-server host 172.20.30.15 non-standard</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>radius-server key string</code></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><code>Switch(config)# radius-server key rad124</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></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><strong>Step 5</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 6</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>
</tbody>
</table>
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><strong>Step 3</strong> aaa user profile  profile-name</td>
<td>Creates a user profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa user profile profile-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa attribute {dnis</td>
<td>clid}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exit Global Configuration mode.</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>Device# debug radius</td>
<td>Displays information associated with RADIUS.</td>
</tr>
<tr>
<td>Device# more</td>
<td>Displays the contents of the current running configuration file. (Note</td>
</tr>
<tr>
<td>system:running-config</td>
<td>that the more system:running-config command has replaced the</td>
</tr>
<tr>
<td></td>
<td>show running-config 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:

Switch(config)# radius-server host host1

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.

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
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):

```
aaa group server radius radgroup1
  server 172.16.1.11
  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:

```
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.

```
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
  Service-Type = Framed-User
  Acct-Session-Id = "00000014"
  Framed-Protocol = PPP
  Framed-IP-Address = 172.16.0.2
  Acct-Input-Octets = 3180
  Acct-Output-Octets = 3186
  Acct-Input-Packets = 40
  Acct-Output-Packets = 40
  Ascend-Connect-Pr = 65
  Acct-Session-Time = 49
  Acct-Delay-Time = 0
  Timestamp = 997190463
  Request-Authenticator = Unverified
```
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:

```
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

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.

```
aaa user profile prfl1
  aaa attribute dnis
```
aaa attribute dnis dnisvalue
no aaa attribute clid
!
Attribute not found.
asa 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 profil
!
!
! debug radius output, which shows that the dnis value has been passed to the radius server.
*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-IE 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
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>
<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>IPv6 commands</td>
<td>• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
<tr>
<td></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 the 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 15.2(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>
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.

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 allows 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:
• 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 CSCu32663, 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.

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 CSCu32663, 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:

Wed Jun 27 04:44:45 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "0000000D"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:45:00 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed-IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:47:46 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed-IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Input-Octets = 3075
Acct-Output-Octets = 167
Acct-Input-Packets = 39
Acct-Output-Packets = 9
Acct-Session-Time = 171
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:45 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "408"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "0000000D"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"

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 Async5 562/4327528 start task_id=35
service=ppp
```

```
Wed Jun 27 04:36:49 2001 172.16.25.15 username1 Async5 562/4327528 stop task_id=35
service=ppp
elapsed_time=51
bytes_in=2844
```

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 562/4327528 start task_id=35
service=ppp
```

```
Wed Jun 27 04:02:25 2001 172.16.25.15 username1 Async5 562/4327528 stop task_id=35
```
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”
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a dial-in user:

```
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-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = “00000006”
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 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
```

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:

```plaintext
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 ip route <cr>
```

The following example shows the information contained in a TACACS+ command accounting record for privilege level 15:

```plaintext
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
```

The following example shows the information contained in a TACACS+ EXEC accounting record for a Telnet user:

```plaintext
start task_id=41 service=shell
stop task_id=41 service=shell elapsed_time=9
```

The following examples show the information contained in a TACACS+ EXEC accounting record for a Telnet user:

```plaintext
NAS-IP-Address = "172.16.25.15"
NAS-Port = 26
User-Name = "username1"
Caller-ID = "10.68.202.158"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000010"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```
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"
```

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"
Acct-Input-Octets = 18686
Acct-Output-Octets = 86
Acct-Input-Packets = 90
Acct-Output-Packets = 68
Acct-Session-Time = 22
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

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 50: Modem Dial-In Call Setup Sequence With Normal Flow and Without Resource Failure Stop Accounting Enabled*
AAA Resource Accounting for Start-Stop Records

The figure below illustrates a call setup sequence with normal call flow (no disconnect) and with AAA resource failure stop accounting enabled.

**Figure 51: 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 52: 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 53: 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.

**Figure 54: Modem Dial-In Call Setup Sequence With Resource Start-Stop Accounting Enabled**

<table>
<thead>
<tr>
<th>Call setup</th>
<th>&quot;Start&quot; record</th>
<th>Modem allocation</th>
<th>Service setup</th>
<th>&quot;Start&quot; record</th>
<th>&quot;Stop&quot; record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call auth</td>
<td>Modem training</td>
<td>User authentication</td>
<td>Call disconnect</td>
<td>&quot;Stop&quot; record</td>
<td></td>
</tr>
</tbody>
</table>

**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.

**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
- Attribute 44, Acct-Session-Id

Accounting messages for a VRRS transitioning out of master state are sent after all PPPoE accounting stop
messages for sessions that are part of that VRRS.
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

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>
<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>
<tr>
<td>IdleTime</td>
<td>The elapsed time in seconds that the session has been idle.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>The session termination object used to disconnect the given client.</td>
</tr>
<tr>
<td>CallId</td>
<td>The entry index corresponding to this accounting session that the Call Tracker record stored.</td>
</tr>
</tbody>
</table>
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>Table 74: SNMP AAA Session Summary</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:

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] 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}
   - ppp accounting {default | list-name}
6. Device(config-line)# end

**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] 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}
   - ppp accounting {default | list-name}
6. Device(config-line)# end

*Note: System accounting does not use named method lists. For system accounting, define only the default method list.*
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</td>
<td></td>
</tr>
<tr>
<td>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>Creates an accounting method list and enables accounting.</td>
</tr>
<tr>
<td>aaa accounting</td>
<td>The argument <em>list-name</em> is a character string used to name the created list.</td>
</tr>
<tr>
<td>{system</td>
<td>network</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>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></td>
</tr>
<tr>
<td>• line [aux</td>
<td>console</td>
</tr>
<tr>
<td>[ending-line-number]</td>
<td></td>
</tr>
<tr>
<td>• interface interface-type interface-number</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>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></td>
</tr>
<tr>
<td>• accounting {arap</td>
<td>commands level</td>
</tr>
<tr>
<td>• ppp accounting</td>
<td>{default</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>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></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>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>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>Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>aaa new-model</code></td>
<td>Enables AAA network security services.</td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>radius-server accounting system host-config</code></td>
<td>Enables the device to send a system accounting record for the addition and deletion of a RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# radius-server accounting system host-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>aaa group server radius server-name</code></td>
<td>Adds the RADIUS server and enters server-group configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa group server radius radgroup1</td>
<td>- The <code>server-name</code> argument specifies the RADIUS server group name.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`server-private {host-name</td>
<td>ip-address} key {0 server-key</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-sg-radius)# server-private 172.16.1.11 key cisco</td>
<td>- (Optional) 0 with the <code>server-key</code> argument specifies that an unencrypted (cleartext) hidden server key follows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) 7 with the <code>server-key</code> argument specifies that an encrypted hidden server key follows.</td>
</tr>
</tbody>
</table>
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>Device(config)# <code>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>Device(config)# <code>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>Device(config)# <code>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:

---
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><code>Device(config)# aaa accounting resource method-list start-stop group server-group</code></td>
<td>Generates a “stop” record for any calls that do not reach user authentication.</td>
</tr>
</tbody>
</table>

**Note** 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.

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>

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:
**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>Device (config)# aaa session-mib disconnect</td>
<td>Monitors and terminates authenticated client connections using SNMP.</td>
</tr>
<tr>
<td></td>
<td>To terminate the call, the disconnect keyword must be used.</td>
</tr>
</tbody>
</table>

**Configuring VRRS Accounting**

Perform the following task to configure Virtual Router Redundancy Service (VRRS) to send AAA Accounting messages to the AAA server:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa accounting vrrs [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>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 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>Step 3 aaa accounting vrrs {default</td>
<td>list-name} start-stop [method1 [method2...]]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa accounting vrrs default start-stop</td>
<td></td>
</tr>
<tr>
<td>Step 4 aaa attribute list list-name</td>
<td>Defines a AAA attribute list locally on a device, and enters attribute list configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa attribute list list1</td>
<td></td>
</tr>
<tr>
<td>Step 5 attribute type name value [service service] [protocol protocol] [mandatory] [tag tag-value]</td>
<td>Defines an attribute type that is to be added to an attribute list locally on a device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-attr-list)# attribute type example 1</td>
<td></td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Exits attribute list configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-attr-list)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 7 vrrs vrrs-group-name</td>
<td>(Optional) Defines a VRRP group and configures parameters for the VRRS group, and enters VRRS configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# vrrs vrrs1</td>
<td></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>
</table>
| Device(config)# no aaa accounting system guarantee-first | The `aaa accounting system guarantee-first` command guarantees system accounting as the first record, which is the default condition.

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 `no aaa accounting system guarantee-first` command can be used.

<table>
<thead>
<tr>
<th>Note</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Entering the <code>no aaa accounting system guarantee-first</code> 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.</td>
<td></td>
</tr>
</tbody>
</table>

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.

```
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
```
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 key_1
   tacacs-server host 172.0.0.1 key key_2
```

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 76: 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>VRRS provides a multiclient 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 614
- 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.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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 default local`
6. `aaa authorization network default 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> enable</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>

| **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 local | Sets the login authentication to use the local username database. The `default` keyword applies the local user database authentication to all ports. |
| **Example:** |         |
| `Switch(config)# aaa authentication login default local` | |

<p>| <strong>Step 5</strong> aaa authorization exec default local | Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell. |
| <strong>Example:</strong> |         |
| <code>Switch(config)# aaa authorization exec default local</code> | |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><code>aaa authorization network default local</code></td>
<td>Configures user AAA authorization for all network-related service requests.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>aaa authorization network default local</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>username name [privilege level] {password encryption-type password}</code></td>
<td>Enters the local database, and establishes a username-based authentication system. Repeat this command for each user.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# <code>username your_user_name privilege 1 password 7 secret567</code></td>
<td></td>
</tr>
<tr>
<td>8</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>Switch(config)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td>10</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>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# <code>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 the 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 Local Authentication and Authorization

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 33

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, on page 615
Prerequisites for Configuring MAC Authentication Bypass, on page 615
Information About MAC Authentication Bypass, on page 616
How to Configure MAC Authentication Bypass, on page 617
Configuration Examples for MAC Authentication Bypass, on page 623
Additional References for MAC Authentication Bypass, on page 623
Feature Information for MAC Authentication Bypass, on page 624

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>0800:2b: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>0800-2b: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>(4, :)</td>
<td>0800:2b86:19de</td>
<td>None</td>
<td>0800:2b86:19de</td>
</tr>
<tr>
<td></td>
<td>(4, -)</td>
<td>0800-2b86-19de</td>
<td></td>
<td>0800-2b86-19de</td>
</tr>
<tr>
<td></td>
<td>(4, .)</td>
<td>0800.2b86.19de</td>
<td></td>
<td>0800.2b86.19de</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>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  *Enter your password if prompted.* |
| Example:  
  
  `Device> enable` | |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:  
  
  `Device# configure terminal` | |
| **Step 3** interface type slot / port | Enters interface configuration mode. |
| Example:  
  
  `Device(config)# interface Gigabitethernet 2/1` | |
| **Step 4** mab | Enables MAB. |
| Example:  
  
  `Device(config-if)# mab` | |
| **Step 5** end | Returns to privileged EXEC mode. |
| Example:  
  
  `Device(config-if)# end` | |
| **Step 6** show authentication sessions interface type slot / port details | Displays the interface configuration and the authenticator instances on the interface. |
| Example:  
  
  `Device# show authentication session interface Gigabitethernet 2/1 details` | |

### 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> 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> 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> interface type slot / port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface Gigabitethernet 2/1</td>
<td></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></td>
<td></td>
</tr>
<tr>
<td>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></td>
<td></td>
</tr>
<tr>
<td>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></td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# authentication port-control auto</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 restart seconds`
10. `end`

**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. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device&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>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>interface type slot / port</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# interface Gigabitethernet 2/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>switchport</td>
<td>Places interface in Layer 2 switched mode.</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></td>
</tr>
<tr>
<td>switchport mode access</td>
<td>Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# switchport mode access</td>
<td></td>
</tr>
<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 violation {restrict</td>
<td>shutdown}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# authentication violation shutdown</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>authentication timer restart seconds</td>
<td>Configures the period of time, in seconds, after which an attempt is made to authenticate an unauthorized port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-if)# authentication timer restart 30</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>
</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>
</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**

   **mab request format attribute 1 groupsize \{1 | 2 | 4 | 12\} separator \{- | : | .\} [lowercase | uppercase]**

   **Example:**
   
   `Device(config)# mab request format attribute 1 groupsize 2 separator :`

   Configures the username format for MAB requests.

| **Step 4**

   **mab request format attribute 2 \{0 | 7\} password**

   **Example:**
   
   `Device(config)# mab request format attribute 2 password1`

   Configures a global password for all MAB requests.

| **Step 5**

   **end**

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

   Returns to privileged EXEC mode.
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>
</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>
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/cfn. An account on Cisco.com is not required.

Table 77: Feature Information for MAC Authentication Bypass

<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 15.2(5)E</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</code>, <code>show dot1x interface</code>.</td>
</tr>
<tr>
<td>Configurable MAB Username and Password</td>
<td>Cisco IOS 15.2(5)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</code>, <code>mab request format attribute 2</code>.</td>
</tr>
</tbody>
</table>
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 625
• Restrictions for Password Strength and Management for Common Criteria, on page 626
• Information About Password Strength and Management for Common Criteria, on page 626
• How to Configure Password Strength and Management for Common Criteria, on page 628
• Configuration Examples for Password Strength and Management for Common Criteria, on page 631
• Additional References for Password Strength and Management for Common Criteria, on page 631
• Feature Information for Password Strength and Management for Common Criteria, on page 632

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>
<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>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:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables AAA globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa common-criteria policy policy-name</td>
<td>Creates the AAA security password policy and enters common criteria configuration policy 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>Device(config)# aaa common-criteria policy policy1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>char-changes number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-cc-policy)# char-changes 4</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>max-length number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-cc-policy)# max-length 25</code></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>min-length number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-cc-policy)# min-length 8</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>numeric-count number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-cc-policy)# numeric-count 4</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>special-case number</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-cc-policy)# special-case 3</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config-cc-policy)# exit</code></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>username username common-criteria-policy policy-name password password</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# username user1 common-criteria-policy policy1 password password1</code></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Device(config)# end</code></td>
</tr>
</tbody>
</table>

(Optional) Specifies the number of changed characters between old and new passwords.

(Optional) Specifies the maximum length of the password.

(Optional) Specifies the minimum length of the password.

(Optional) Specifies the number of numeric characters in the password.

(Optional) Specifies the number of special characters in the password.

(Optional) Exits common criteria configuration policy mode and returns to global configuration mode.

(Optional) Applies a specific policy and password to a user profile.

Returns to privileged EXEC mode.
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>

**RFCs**

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2865</td>
<td>Remote Authentication Dial-in User Service</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.

Table 78: Feature Information for Password Strength and Management for Common Criteria

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Strength and Management for Common Criteria</td>
<td>Cisco IOS 15.2(5)E</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 633
• Prerequisites for AAA-SERVER-MIB Set Operation, on page 633
• Restrictions for AAA-SERVER-MIB Set Operation, on page 634
• Information About AAA-SERVER-MIB Set Operation, on page 634
• How to Configure AAA-SERVER-MIB Set Operation, on page 634
• Configuration Examples for AAA-SERVER-MIB Set Operation, on page 635
• Additional References for AAA-SERVER-MIB Set Operation, on page 637
• Feature Information for AAA-SERVER-MIB Set Operation, on page 638

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

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><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device&gt; enable</td>
</tr>
</tbody>
</table>
|                   | Enables privileged EXEC mode.  
|                   | • Enter your password if prompted. |
| **Step 2**       | **show running-config | include radius-server host**<br>**Example:**<br>Device# show running-config | include radius-server host |
|                   | Displays all the RADIUS servers that are configured in the global configuration mode. |
| **Step 3**       | **show aaa servers**<br>**Example:**<br>Device# show aaa servers |
|                   | Displays information about the number of requests sent to and received from authentication, authorization, and accounting (AAA) servers. |

**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.<br>radius-server host 172.19.192.238 auth-port 2095 acct-port 2096 key cisco2  
! The following line is for server 2.<br>radius-server host 172.19.192.238 auth-port 1645 acct-port 1646

**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  
Authen: request 8, timeouts 8  
Response: unexpected 0, server error 0, incorrect 0, time 0ms  
Transaction: success 0, failure 2  
Author: request 0, timeouts 0
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 -i 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>
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/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></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 79: 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(5)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>
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 rexec and rsh tools. Two versions of SSH are available: SSH Version 1 and SSH Version 2.

- Finding Feature Information, on page 639
- Prerequisites for Configuring Secure Shell, on page 639
- Restrictions for Configuring Secure Shell, on page 640
- Information About Configuring Secure Shell, on page 640
- How to Configure Secure Shell, on page 643
- Configuration Examples for Secure Shell, on page 654
- Additional References for Secure Shell, on page 655
- Feature Information for Configuring Secure Shell, on page 656

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.

• 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 Configuring Secure Shell

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>
</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**
  hostname hostname
  Example: |
<p>| Configures a hostname and IP domain name for your Switch. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# hostname your_hostname</td>
<td>Note Follow this procedure only if you are configuring the Switch as an SSH server.</td>
</tr>
<tr>
<td>Step 4 ip domain-name domain_name</td>
<td>Configures a host domain for your Switch.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip domain-name your_domain</td>
<td></td>
</tr>
<tr>
<td>Step 5 crypto key generate rsa</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. 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. Note Follow this procedure only if you are configuring the Switch as an SSH server.</td>
</tr>
<tr>
<td>Example: Switch(config)# crypto key generate rsa</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>

### Configuring the SSH Server

Follow these steps to configure the SSH server:

*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 vty line_number [ending_line_number]
   • transport input ssh
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:
| Switch> enable    | • Enter your password if prompted. |
| **Step 2**
| configure terminal| Enters global configuration mode. |
| Example:
| Switch# configure terminal |
| **Step 3**
| ip ssh version [1 | 2] | (Optional) Configures the Switch to run SSH Version 1 or SSH Version 2. |
| Example:
| Switch(config)# ip ssh version 1 | • 1—Configure the Switch to run SSH Version 1. |
|                     | • 2—Configure the Switch to run SSH Version 2. |
|                     | 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. |
| **Step 4**
| ip ssh {timeout seconds | authentication-retries number} | Configures the SSH control parameters: |
| Example:
<p>| Switch(config)# ip ssh timeout 90 authentication-retries 2 | • 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. 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 |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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></td>
<td>Repeat this step when configuring both parameters.</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.

**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>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>• Enter your password if prompted.</td>
</tr>
<tr>
<td></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></td>
<td><code>line line-number ending-line-number</code></td>
<td>Identifies a line for configuration and enters line 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>
<tr>
<td>Device# line 1 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no exec</td>
<td>Enables EXEC processing on a line.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# no exec</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> login authentication listname</td>
<td>Defines a login authentication mechanism for the lines.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# login authentication default</td>
<td></td>
<td></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>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# transport input ssh</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits line configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device(config)# exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> ssh -l userid : {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>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device# ssh -l lab:1 router.example.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

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>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 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>Step 3 line line-number ending-line-number</td>
<td>Identifies a line for configuration and enters line configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# line 1 200</td>
<td></td>
</tr>
<tr>
<td>Step 4 no exec</td>
<td>Disables EXEC processing on a line.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-line)# no exec</td>
<td></td>
</tr>
<tr>
<td>Step 5 login authentication listname</td>
<td>Defines a login authentication mechanism for the lines.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note The authentication method must use a username and password.</td>
</tr>
<tr>
<td>Device(config-line)# login authentication default</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>rotary group</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-line)# rotary 1</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>transport input ssh</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-line)# transport input ssh</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>exit</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config-line)# exit</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>exit</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# exit</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>ssh -l userid :rotary {number} {ip-address}</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# ssh -l lab:rotary1 router.example.com</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
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`

**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>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>debug ip ssh client</code></td>
<td>Displays debugging messages for the SSH client.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# debug ip ssh client</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>show ssh</code></td>
<td>Displays the status of the SSH server connections.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show ssh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>show line</code></td>
<td>Displays parameters of a terminal line.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show line</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 80: Commands for Displaying 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... ]]
6. username name [privilege level] password encryption-type encrypted-password
7. ip scp server enable
8. exit
9. show running-config
10. debug ip scp

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</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>
<tr>
<td>Step 2</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>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# aaa new-model</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><strong>Step 4</strong></td>
<td>`aaa authentication login {default</td>
<td>list-name} method1 [ method2... ]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>aaa authentication login default group tacacs+</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`aaa authorization {network</td>
<td>exec</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <code>exec</code> keyword runs authorization to determine if the user is allowed to run an EXEC shell; therefore, you must use the <code>exec</code> keyword when you configure SCP.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>aaa authorization exec default group tacacs+</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>username name [privilege level] password encryption-type encrypted-password</code></td>
<td>Establishes a username-based authentication system.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You may omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>username superuser privilege 2 password 0 superpassword</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>ip scp server enable</code></td>
<td>Enables SCP server-side functionality.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>ip scp server enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>exit</code></td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# <code>exit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>show running-config</code></td>
<td>(Optional) Displays the SCP server-side functionality.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>debug ip scp</code></td>
<td>(Optional) Troubleshoots SCP authentication problems.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# <code>debug ip scp</code></td>
<td></td>
</tr>
</tbody>
</table>
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
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**

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:

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:

```
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:

```
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:

```
Device# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following example shows that SSH is disabled:

```
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 Session Started guest
```

The following example shows that SSH is disabled:

```
Device# show ssh
%No SSH server connections running.
```

Additional References for Secure Shell

<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>
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 Configuring Secure Shell

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 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-EId. The following command was introduced: ssh.</td>
</tr>
</tbody>
</table>
CHAPTER 37

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 657
- Information About Secure Shell Version 2 Support, on page 657
- How to Configure Secure Shell Version 2 Support, on page 660
- Configuration Examples for Secure Shell Version 2 Support, on page 675
- Additional References for Secure Shell Version 2 Support, on page 680
- Feature Information for Secure Shell Version 2 Support, on page 680

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.
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.

The login banner is supported in SSH Version 2, but it is not supported in Secure Shell Version 1.

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.

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.
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.

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*.

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
tcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
tcpConnEntry.1.10.0.0.1.22.10.0.0.2.55246 = 1056
tcpConnEntry.2.10.0.0.1.22.10.0.0.2.55246 = 1392
local.9.2.1.18.2 = lab
```
**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> 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>
</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

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 3 | hostname *name*  
Example:  
Device(config)# hostname cisco7200 | Configures a hostname for your device. |
| Step 4 | ip domain-name *name*  
Example:  
cisco7200(config)# ip domain-name example.com | Configures a domain name for your device. |
| Step 5 | crypto key generate rsa  
Example:  
cisco7200(config)# crypto key generate rsa | Enables the SSH server for local and remote authentication. |
| Step 6 | ip ssh [time-out *seconds* | authentication-retries *integer*]  
Example:  
cisco7200(config)# ip ssh time-out 120 | (Optional) Configures SSH control variables on your device. |
| Step 7 | ip ssh version [1 | 2]  
Example:  
cisco7200(config)# ip ssh version 1 | (Optional) Specifies the version of SSH to be run on your device. |
| Step 8 | exit  
Example:  
cisco7200(config)# exit | Exits global configuration mode and enters privileged EXEC mode.  
• Use no hostname command to return to the default host. |
### 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><em>enable</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></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><em>configure terminal</em></td>
<td></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>Specifies the RSA key pair to be used for SSH.</td>
</tr>
<tr>
<td><em>ip ssh rsa keypair-name keypair-name</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>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></td>
<td>Enables the SSH server for local and remote authentication on the device.</td>
</tr>
<tr>
<td><em>crypto key generate rsa usage-keys label key-label modulus modulus-size</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>For SSH Version 2, the modulus size must be at least 768 bits.</td>
</tr>
<tr>
<td>Device(config)# crypto key generate rsa usage-keys label sshkeys modulus 768</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures SSH control variables on your device.</td>
</tr>
<tr>
<td>*ip ssh [time-out seconds</td>
<td>authentication-retries integer]*</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip ssh time-out 12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies the version of SSH to be run on the device.</td>
</tr>
<tr>
<td><em>ip ssh version 2</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip ssh version 2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Exits global configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td><em>exit</em></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(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><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device&gt; 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><strong>Example:</strong> <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>hostname name</code></td>
<td>Specifies the hostname.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Device(config)# hostname host1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip domain-name name</code></td>
<td>Defines a default domain name that the Cisco software uses to complete unqualified hostnames.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>host1(config)# ip domain-name name1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>crypto key generate rsa</code></td>
<td>Generates RSA key pairs.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>host1(config)# crypto key generate rsa</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>ip ssh pubkey-chain</code></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><strong>Example:</strong> <code>host1(config)# ip ssh pubkey-chain</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<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>
</tbody>
</table>

| Step 7 | username  
| Example: | username |
| host1(conf-ssh-pubkey)# username user1 | Configures the SSH username and enters public-key user configuration mode. |

| Step 8 | key-string  
| Example: | key-string |
| host1(conf-ssh-pubkey-user)# key-string | Specifies the RSA public key of the remote peer and enters public-key data configuration mode. |

| Note | You can obtain the public key value from an open SSH client; that is, from the .ssh/id_rsa.pub file. |

| Step 9 | key-hash  key-type  key-name  
| Example: | key-hash ssh-rsa key1 |
| host1(conf-ssh-pubkey-data)# key-hash ssh-rsa key1 | (Optional) Specifies the SSH key type and version. |

| • 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. |

| Note | 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. |

| Step 10 | end  
| Example: | end |
| host1(conf-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
### 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></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>configure terminal</td>
<td></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>hostname <strong>name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# hostname host1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>ip domain-name <strong>name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>host1(config)# ip domain-name name1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>host1(config)# crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>ip ssh pubkey-chain</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>host1(config)# ip ssh pubkey-chain</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>server <strong>server-name</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the Cisco IOS SSH Client to Perform RSA-Based Server Authentication

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1(conf-ssh-pubkey)# server server1</td>
<td>Specifies the RSA public-key of the remote peer and enters public key data configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 8** key-string  
Example:  
host1(conf-ssh-pubkey-server)# key-string | You can obtain the public key value from an open SSH client; that is, from the .ssh/id_rsa.pub file. |
| **Step 9** exit  
Example:  
host1(conf-ssh-pubkey-data)# exit | Exits public-key data configuration mode and enters public-key server configuration mode. |
| **Step 10** key-hash  
key-type  
key-name  
Example:  
host1(conf-ssh-pubkey-server)# key-hash ssh-rsa key1 | (Optional) Specifies the SSH key type and version.  
• 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. |
| **Step 11** end  
Example:  
host1(conf-ssh-pubkey-server)# end | Exits public-key server configuration mode and returns to privileged EXEC mode. |
| **Step 12** configure terminal  
Example:  
host1# configure terminal | Enters global configuration mode. |
| **Step 13** ip ssh stricthostkeycheck  
Example:  
host1(config)# ip ssh stricthostkeycheck | Ensures that server authentication takes place.  
• The connection is terminated in case of a failure.  
• Use no hostname command to return to the default host. |
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}]
   | [-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>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Starts an encrypted session with a remote networking device.</td>
</tr>
</tbody>
</table>

Example:
Device# ssh -v 2 -c aes256-ctr -m hmac-sha1-96 -l user2 10.76.82.24

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 defaultlocal
6. username name privilege privilege-level password password
7. ip ssh time-out seconds
8. ip ssh authentication-retries integer
### 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><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</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><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>aaa new-model</code></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>aaa authentication login default local</code></td>
<td>Sets AAA authentication at login to use the local username database for authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa authentication login default local</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>aaa authorization exec 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>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# aaa authorization exec default local</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>username name privilege privilege-level password password</code></td>
<td>Establishes a username-based authentication system, and specifies the username, privilege level, and an unencrypted password.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# username samplename privilege 15 password password1</td>
<td>Note: The minimum value for the <code>privilege-level</code> argument is 15. A privilege level of less than 15 results in the connection closing.</td>
</tr>
<tr>
<td>7</td>
<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>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip ssh time-out 120</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>ip ssh authentication-retries integer</code></td>
<td>Sets the number of authentication attempts after which the interface is reset.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

Device(config)# ip ssh authentication-retries 3

**Step 9**

**ip scpserverenable**

**Example:**

Device(config)# ip scp server enable

**Step 10**

**exit**

**Example:**

Device(config)# exit

**Step 11**

**debug ip scp**

**Example:**

Device# debug ip scp

### 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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></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>Displays the status of SSH server connections.</td>
</tr>
<tr>
<td>show ssh</td>
<td></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>Exits privileged EXEC mode and returns to user EXEC mode.</td>
</tr>
<tr>
<td>exit</td>
<td></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:

```
Device# show ssh
Connection Version Encryption State Username
0 1.5 3DES Session started lab
Connection Version Mode Encryption Hmac State Username
Username
1 2.0 IN aes128-cbc hmac-md5 Session started lab
1 2.0 OUT aes128-cbc hmac-md5 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:

```
Device# show ssh
Connection Version Mode Encryption Hmac State Username
Username
1 2.0 IN aes128-cbc hmac-md5 Session started lab
1 2.0 OUT aes128-cbc hmac-md5 Session started lab
%No SSHv1 server connections running.
```

The following sample output from the `show ssh` command displays status of various SSH Version 1 and Version 2 connections for a Version 1 connection with no Version 2 connection:

```
Device# show ssh
Connection Version Encryption State Username
0 1.5 3DES Session started lab
%No SSHv2 server connections running.
```

Verifying the Secure Shell Status

SUMMARY STEPS

1. enable
2. show ip ssh
3. exit

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>
### Command or Action

**Example:**

Device> enable

**Step 2**

**show ip ssh**

**Example:**

Device# show ip ssh

**Step 3**

**exit**

**Example:**

Device# exit

### 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:

```
Device# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

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 a Version 2 connection with no Version 1 connection:

```
Device# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

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 a Version 1 connection with no Version 2 connection:

```
Device# show ip ssh
3d06h: %SYS-5-CONFIG_I: Configured from console by console
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```
## 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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> debug ip ssh</td>
<td>Enables debugging of SSH.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# debug ip ssh</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> debug snmp packet</td>
<td>Enables debugging of every SNMP packet sent or received by the device.</td>
</tr>
<tr>
<td><strong>Example:</strong> 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: kexderive_keys complete
00:33:55: SSH2 1: send: len 16 (includes padlen 10)
00:33:55: SSH2 1: newkeys: mode 1
00:33:55: SSH2 1: SSH2_MSG_NEWKEYS sent
00:33:55: SSH2 1: waiting for SSH2_MSG_NEWKEYS
00:33:55: SSH2 1: ssh_receive: 16 bytes received
00:33:55: SSH2 1: input: packet len 16
00:33:55: SSH2 1: partial packet 8, need 8, maclen 0
00:33:55: SSH2 1: input: packet len 10
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
00:33:55: 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 48, 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)
00:33:56: 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-req 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-req 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: 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
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 #9
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 #13 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 #10
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #14 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 17)
00:34:08: SSH2 1: done calc MAC out #11
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #15 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 16)
00:34:08: SSH2 1: done calc MAC out #12
00:34:08: SSH2 1: ssh_receive: 48 bytes received
00:34:08: SSH2 1: input: packet len 32
00:34:08: SSH2 1: partial packet 16, need 16, maclen 16
00:34:08: SSH2 1: MAC #16 ok
00:34:08: SSH2 1: input: padlen 17
00:34:08: SSH2 1: received packet type 94
00:34:08: SSH2 1: send: len 32 (includes padlen 16)
00:34:08: SSH2 1: done calc MAC out #13
00:34:08: SSH2 1: send: len 48 (includes padlen 18)
00:34:08: SSH2 1: done calc MAC out #14
00:34:08: SSH2 1: send: len 16 (includes padlen 6)
00:34:08: SSH2 1: done calc MAC out #15
00:34:08: SSH1: Session terminated normally
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.

Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username samplename privilege 15 password password1
Device(config)# ip ssh time-out 120
Device(config)# ip ssh authentication-retries 3
Device(config)# ip scp server enable

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
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:
*Nov 17 12:50:53.199: SSH0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: sent protocol version id SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.199: SSH CLIENT0: protocol version exchange successful
*Nov 17 12:50:53.203: SSH0: protocol version id is - SSH-1.99-Cisco-1.25
*Nov 17 12:50:53.335: SSH CLIENT0: key exchange successful and encryption on
*Nov 17 12:50:53.335: SSH2 CLIENT 0: using method keyboard-interactive
Password:
Password:
Password:
*Nov 17 12:51:01.887: SSH2 CLIENT 0: using method password authentication
Password:
Password: lab
Device2>

*Nov 17 12:51:11.407: SSH2 CLIENT 0: SSH2_MSG_USERAUTH_SUCCESS message received
*Nov 17 12:51:11.407: SSH CLIENT0: user authenticated
*Nov 17 12:51:11.407: SSH2 CLIENT 0: pty-req request sent
*Nov 17 12:51:11.411: SSH2 CLIENT 0: shell request sent
*Nov 17 12:51:11.411: SSH CLIENT0: session open
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: cisco
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.
New Password: cisco123
Re-enter New password: cisco123
Device2> exit
[Connection to 10.1.1.3 closed by foreign host]
Device1# ssh -l cisco 10.1.1.3
Password: cisco1
Your password has expired.
Enter a new one now.
New Password: cisco
Re-enter New password: cisco12
The New and Re-entered passwords have to be the same.
Try again.
New Password: cisco
Re-enter New password: cisco
Device2>
```

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.

```
Device# ssh -l cisco 10.1.1.3
Password: cisco
Device2> exit
```
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#

*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.110.0.0.1.22.10.0.0.2.55246 = 4
  ltcpConnEntry.5.10.0.0.1.22.10.0.0.2.55246 = 1015
  ltcpConnEntry.110.0.0.1.22.10.0.0.2.55246 = 1056
  ltcpConnEntry.2.10.0.0.1.22.10.0.0.2.55246 = 1392
  local.9.2.1.18.2 = lab
*Jul 18 10:18:42.879: SNMP: Packet sent via UDP to 10.0.0.2

Device1#
```

Examples: 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
```
The following is sample output from the `debug ip ssh packet` command. The output provides debugging information about the SSH packet.

```plaintext
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: 24 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: 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: 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: ssh_receive: 16 bytes received
00:05:43: SSH2 0: partial packet length(block size)8 bytes,needed 8 bytes, maclen 0
00:05:43: SSH2 0: ssh_receive: 8 bytes received
00:05:43: SSH2 0: ssh_receive: 52 bytes received
00:05:43: SSH2 0: input: padlength 6 bytes
00:05:43: SSH2 0: signature length 143
00:05:43: SSH2 0: send:packet of length 448 (length also includes padlen of 7)
00:05:43: SSH2 0: send:packet of length 16 (length also includes padlen of 10)
00:05:43: SSH2 0: newkeys: mode 1
00:05:43: SSH2 0: ssh_receive: 16 bytes received
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: input: padlength 10 bytes
00:05:43: SSH2 0: newkeys: mode 1
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

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>

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. An account on Cisco.com is not required.

Table 81: 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 Release 15.2(5)E</td>
<td>The Cisco image was updated to provide for the automatic generation of SNMP traps when an SSH session terminates.</td>
</tr>
</tbody>
</table>
CHAPTER 38

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 681
- Prerequisites for X.509v3 Certificates for SSH Authentication, on page 681
- Restrictions for X.509v3 Certificates for SSH Authentication, on page 682
- Information About X.509v3 Certificates for SSH Authentication, on page 682
- How to Configure X.509v3 Certificates for SSH Authentication, on page 683
- Verifying the Server and User Authentication Using Digital Certificates, on page 686
- Configuration Examples for X.509v3 Certificates for SSH Authentication, on page 691
- Additional References for X.509v3 Certificates for SSH Authentication, on page 691
- Feature Information for X.509v3 Certificates for SSH Authentication, on page 692

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:
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

- 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.

### 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. ocs-pro-response include
8. end
9. line vty line_number [ending_line_number]
10. transport input ssh

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>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Switch> enable
Switch# configure terminal
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** ip ssh server algorithm hostkey \{x509v3-ssh-rsa [ssh-rsa] | ssh-rsa [x509v3-ssh-rsa]\} | Defines the order of host key algorithms. Only the configured algorithm is negotiated with the Secure Shell (SSH) client.  
  **Note** 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 |
| **Example:**  
  Switch(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa | |
| **Step 4** ip ssh server certificate profile | Configures server and user certificate profiles and enters SSH certificate profile configuration mode. |
| **Example:**  
  Switch(config)# ip ssh server certificate profile | |
| **Step 5** server | Configures server certificate profile and enters SSH server certificate profile server configuration mode.  
  - The server profile is used to send out the certificate of the server to the SSH client during server authentication. |
| **Example:**  
  Switch(ssh-server-cert-profile)# server | |
| **Step 6** trustpoint sign PKI-trustpoint-name | Attaches the public key infrastructure (PKI) trustpoint to the server certificate profile.  
  - The SSH server uses the certificate associated with this PKI trustpoint for server authentication. |
| **Example:**  
  Switch(ssh-server-cert-profile-server)# trustpoint sign trust1 | |
| **Step 7** ocsp-response include | (Optional) Sends the Online Certificate Status Protocol (OCSP) response or OCSP stapling along with the server certificate.  
  **Note** By default, no OCSP response is sent along with the server certificate. |
| **Example:**  
  Switch(ssh-server-cert-profile-server)# ocsp-response include | |
| **Step 8** end | Exits SSH server certificate profile server configuration mode and returns to privileged EXEC mode. |
| **Example:**  
  Switch(ssh-server-cert-profile-server)# end | |
| **Step 9** line vty line_number [ending_line_number] | 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. |
| **Example:**  
  Switch(config)# line vty line_number [ending_line_number] | |
| **Step 10** transport input ssh | Specifies that the Switch prevent non-SSH Telnet connections. This limits the router to only SSH connections. |
| **Example:**  
  Switch(config-line)#transport input ssh | |
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. ocs-rp response required
9. end
10. line vty line_number [ending_line_number]
11. transport input ssh

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 authentication {publickey</td>
<td>keyboard</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ip ssh server algorithm authentication publickey</td>
<td>• The IOS SSH server must have at least one configured user authentication algorithm.</td>
</tr>
<tr>
<td></td>
<td>• To use the certificate method for user authentication, the publickey keyword must be configured.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip ssh server algorithm publickey {x509v3-ssh-rsa [ssh-rsa]</td>
<td>ssh-rsa [x509v3-ssh-rsa]}</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ip ssh server algorithm publickey x509v3-ssh-rsa</td>
<td><strong>Note</strong> The IOS SSH client must have at least one configured public key algorithm:</td>
</tr>
<tr>
<td></td>
<td>• x509v3-ssh-rsa—Certificate-based authentication</td>
</tr>
<tr>
<td></td>
<td>• ssh-rsa—Public-key-based authentication</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 5**  
*ip ssh server certificate profile*  
**Example:**  
```
Switch(config)# ip ssh server certificate profile
```
Configures server certificate profile and user certificate profile and enters SSH certificate profile configuration mode.

**Step 6**  
*user*  
**Example:**  
```
Switch(ssh-server-cert-profile)# user
```
Configures user certificate profile and enters SSH server certificate profile user configuration mode.

**Step 7**  
*trustpoint verify PKI-trustpoint-name*  
**Example:**  
```
Switch(ssh-server-cert-profile-user)# trustpoint verify trust2
```
Configures the public key infrastructure (PKI) trustpoint that is used to verify the incoming user certificate.  
**Note**  
Configure multiple trustpoints by executing the same command multiple times. A maximum of 10 trustpoints can be configured.

**Step 8**  
*ocsp-response required*  
**Example:**  
```
Switch(ssh-server-cert-profile-user)# ocsp-response required
```
(Optional) Mandates the presence of the Online Certificate Status Protocol (OCSP) response with the incoming user certificate.  
**Note**  
By default, the user certificate is accepted without an OCSP response.

**Step 9**  
*end*  
**Example:**  
```
Switch(ssh-server-cert-profile-user)# end
```
Exits SSH server certificate profile user configuration mode and returns to privileged EXEC mode.

**Step 10**  
*line vty line_number [ending_line_number]*  
**Example:**  
```
Switch(config)# line vty line_number [ending_line_number]
```
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.

**Step 11**  
*transport input ssh*  
**Example:**  
```
Switch(config-line)#transport input ssh
```
Specifies that the Switch prevent non-SSH Telnet connections. This limits the router to only SSH connections.

---

### Verifying the Server and User Authentication Using Digital Certificates

**SUMMARY STEPS**

1. enable  
2. show ip ssh
3. debug ip ssh detail
4. show log
5. debug ip packet
6. show log

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
Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa
Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits

Step 3  debug ip ssh detail

Turns on debugging messages for SSH details.

Example:

Device# debug ip ssh detail

ssh detail messages debugging is on

Step 4  show log

Shows the debug message log.

Example:

Device# show log

Syslog logging: enabled (0 messages dropped, 9 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.
No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging: level debugging, 233 messages logged, xml disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
File logging: disabled
Persistent logging: disabled

No active filter modules.

Trap logging: level informational, 174 message lines logged
Logging Source-Interface: VRF Name:
Log Buffer (4096 bytes):
5 IST: SSH2 CLIENT 0: SSH2_MSG_KEXINIT sent
*Sep 6 14:44:08.496 IST: SSH0: protocol version id is = SSH-1.99-Cisco-1.25
*Sep 6 14:44:08.496 IST: SSH2 0: kexinit sent: kex algo = diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1
*Sep 6 14:44:08.496 IST: SSH2 0: Server certificate trustpoint not found. Skipping hostkey algo = x509v3-ssh-rsa
*Sep 6 14:44:08.496 IST: SSH2 0: kexinit sent: hostkey algo = ssh-rsa
*Sep 6 14:44:08.496 IST: SSH2 0: kexinit sent: encryption algo = aes128-ctr,aes192-ctr,aes256-ctr
*Sep 6 14:44:08.496 IST: SSH2 0: kexinit sent: mac algo = hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96
*Sep 6 14:44:08.496 IST: SSH2 0: SSH2_MSG_KEXINIT sent
*Sep 6 14:44:08.496 IST: SSH2 0: SSH2_MSG_KEXINIT received
*Sep 6 14:44:08.496 IST: SSH2 0: kex: client->server enc:aes128-ctr mac:hmac-sha2-256
*Sep 6 14:44:08.496 IST: SSH2 0: kex: server->client enc:aes128-ctr mac:hmac-sha2-256
*Sep 6 14:44:08.496 IST: SSH2 0: Using hostkey algo = ssh-rsa
*Sep 6 14:44:08.496 IST: SSH2 0: Using kex algo = diffie-hellman-group-exchange-sha1
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: SSH2_MSG_KEXINIT received
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: kex: server->client enc:aes128-ctr mac:hmac-sha2-256
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: kex: client->server enc:aes128-ctr mac:hmac-sha2-256
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: Using hostkey algo = ssh-rsa
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: Using kex algo = diffie-hellman-group-exchange-sha1
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: SSH2_MSG_KEX_DH_GEX_REQUEST sent
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: Range sent- 2048 < 2048 < 4096
*Sep 6 14:44:08.497 IST: SSH2 CLIENT 0: SSH2_MSG_KEX_DH_GEX_REQUEST received
*Sep 6 14:44:08.497 IST: SSH2 0: Range sent by client is - 2048 < 2048 < 4096
*Sep 6 14:44:08.497 IST: SSH2 0: Modulus size established : 2048 bits
*Sep 6 14:44:08.510 IST: SSH2 0: expecting SSH2_MSG_KEX_DH_GEX_INIT
*Sep 6 14:44:08.510 IST: SSH2 CLIENT 0: SSH2_MSG_KEX_DH_GEX_GROUP received
*Sep 6 14:44:08.510 IST: SSH2 CLIENT 0: Server has chosen 2048 -bit dh keys
*Sep 6 14:44:08.523 IST: SSH2 CLIENT 0: expecting SSH2_MSG_KEX_DH_GEX_REPLY
*Sep 6 14:44:08.524 IST: SSH2 0: SSH2_MSG_KEX_DH_GEX_INIT received
*Sep 6 14:44:08.555 IST: SSH2: kex_derive_keys complete
*Sep 6 14:44:08.555 IST: SSH2 0: SSH2_MSG_NEWKEYS sent
*Sep 6 14:44:08.555 IST: SSH2 0: waiting for SSH2_MSG_NEWKEYS
*Sep 6 14:44:08.555 IST: SSH2 CLIENT 0: SSH2_MSG_KEX_DH_GEX_REPLY received
*Sep 6 14:44:08.555 IST: SSH2 CLIENT 0: Skipping ServerHostKey Validation
*Sep 6 14:44:08.571 IST: SSH2 0: signature length 271
*Sep 6 14:44:08.571 IST: SSH2 0: kex_derive_keys complete
*Sep 6 14:44:08.571 IST: SSH2 0: SSH2_MSG_NEWKEYS sent
*Sep 6 14:44:08.571 IST: SSH2 0: waiting for SSH2_MSG_NEWKEYS
*Sep 6 14:44:08.571 IST: SSH2 0: SSH2_MSG_NEWKEYS received
*Sep 6 14:44:08.571 IST: SSH2 0: SSH2_MSG_NEWKEYS received
*Sep 6 14:44:08.571 IST: SSH2 0: Authentications that can continue = publickey,keyboard-interactive,password
*Sep 6 14:44:08.572 IST: SSH2 0: Using method = none
*Sep 6 14:44:08.572 IST: SSH2 0: Authentications that can continue =
publickey,keyboard-interactive,password
*Sep 6 14:44:08.572 IST: SSH2 0: Using method = keyboard-interactive
*Sep 6 14:44:11.983 IST: SSH2 0: authentication successful for cisco
*Sep 6 14:44:11.984 IST: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: 192.168.121.40] [localport: 22] at 14:44:11 IST Thu Sep 6 2018
*Sep 6 14:44:11.984 IST: SSH2 0: channel open request
*Sep 6 14:44:11.985 IST: SSH2 0: pty-req request
*Sep 6 14:44:11.985 IST: SSH2 0: setting TTY - requested: height 24, width 80; set: height 24, width 80
*Sep 6 14:44:11.985 IST: SSH2 0: shell request
*Sep 6 14:44:11.985 IST: SSH2 0: shell message received
*Sep 6 14:44:11.985 IST: SSH2 0: starting shell for vty
*Sep 6 14:44:22.066 IST: %SYS-6-LOGOUT: User cisco has exited tty session 1(192.168.121.40)
*Sep 6 14:44:22.166 IST: SSH0: Session terminated normally
*Sep 6 14:44:22.167 IST: SSH CLIENT0: Session terminated normally

Step 5  debug ip packet

Turns on debugging for IP packet details.

Example:

Device# debug ip packet

Step 6  show log

Shows the debug message log.

Example:

Device# show log

yslog logging: enabled (0 messages dropped, 9 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging: level debugging, 1363 messages logged, xml disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
File logging: disabled
Persistent logging: disabled

No active filter modules.

Trap logging: level informational, 176 message lines logged
Logging Source-Interface: VRF Name:

Log Buffer (4096 bytes):
bleid=0, s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.177 IST: IP: s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), len 40, sending
*Sep 6 14:45:45.177 IST: IP: s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), len 40, output feature, NAT Inside(8), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
Verifying the Server and User Authentication Using Digital Certificates

*Sep 6 14:45:45.177 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.177 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.177 IST: IP: s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40, len 40, local feature, feature skipped, NAT(2), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:45:45.178 IST: IP: tableid=0, s=192.168.121.40 (local), d=192.168.121.40, len 40, local feature, feature skipped, NAT(2), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:45:45.178 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.178 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.178 IST: IP: s=192.168.121.40 (local), d=192.168.121.40, len 40, local feature, feature skipped, NAT(2), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40, len 40, sending
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40, d=192.168.121.40 (FortyGigabitEthernet1/0/1), len 40, output feature, NAT Inside(8), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40, len 40,本地特征，特征跳过，NAT(2)子网，rtype 1，forus FALSE，sendself FALSE，mtu 0，fwdchk FALSE
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40 (local), d=192.168.121.40, len 40, local feature, feature skipped, NAT(2), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40, len 40, sending
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40, d=192.168.121.40 (FortyGigabitEthernet1/0/1), len 40, output feature, NAT Inside(8), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40, len 40,本地特征，特征跳过，NAT(2)子网，rtype 1，forus FALSE，sendself FALSE，mtu 0，fwdchk FALSE
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40 (local), d=192.168.121.40, len 40, local feature, feature skipped, NAT(2), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:45:45.179 IST: IP: tableid=0, s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:45:45.179 IST: IP: s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:44:45.178 IST: IP: s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40, len 40, sending
*Sep 6 14:44:45.178 IST: IP: s=192.168.121.40, d=192.168.121.40 (FortyGigabitEthernet1/0/1), len 40, output feature, NAT Inside(8), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:44:45.178 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40, len 40,本地特征，特征跳过，NAT(2)子网，rtype 1，forus FALSE，sendself FALSE，mtu 0，fwdchk FALSE
*Sep 6 14:44:45.178 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:44:45.178 IST: IP: tableid=0, s=192.168.121.40 (FortyGigabitEthernet1/0/1), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
*Sep 6 14:44:45.178 IST: IP: s=192.168.121.40 (local), d=192.168.121.40, len 40, local feature, feature skipped, NAT(2), rtype 1, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 6 14:44:45.178 IST: IP: tableid=0, s=192.168.121.40 (local), d=192.168.121.40 (FortyGigabitEthernet1/0/1), routed via RIB
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 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>
<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 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 |
Security

Feature Information for X.509v3 Certificates for SSH Authentication
CHAPTER 39

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 695
• Information About Secure Socket Layer HTTP, on page 695
• Monitoring Secure HTTP Server and Client Status, on page 706
• Configuration Examples for Secure Socket Layer HTTP, on page 706
• Additional References for Secure Socket Layer HTTP, on page 707
• Feature Information for Secure Socket Layer HTTP, on page 707
• Glossary, on page 708

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

<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
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

or

https://host.domain.com:1026

The existing **ip http access-class access-list-number** command for specifying the access-list (Only IPv4 ACLs) is going to be deprecated. You can still use this command to specify an access list to allow access to the HTTP server. Two new commands have been introduced to enable support for specifying IPv4 and IPv6 ACLs. These are **ip http access-class ipv4 access-list-name | access-list-number** for specifying IPv4 ACLs and **ip http access-class ipv6 access-list-name** for specifying IPv6 ACLs. We recommend using the new CLI to avoid receiving warning messages.

Note the following considerations for specifying access-lists:

- If you specify an access-list that does not exist, the configuration takes place but you receive the below warning message:

  ACL being attached does not exist, please configure it

- If you use the **ip http access-class** command for specifying an access-list for the HTTP server, the below warning message appears:

  This CLI will be deprecated soon, Please use new CLI ip http access-class ipv4/ipv6 <access-list-name>| <access-list-number>

- If you use **ip http access-class ipv4 access-list-name | access-list-number** or **ip http access-class ipv6 access-list-name**, and an access-list was already configured using **ip http access-class**, the below warning message appears:

  Removing ip http access-class <access-list-number>
ip http access-class access-list-number and ip http access-class ipv4 access-list-name | access-list-number share the same functionality. Each command overrides the configuration of the previous command. The following combinations between the configuration of the two commands explain the effect on the running configuration:

- If ip http access-class access-list-number is already configured and you try to configure using ip http access-class ipv4 access-list-number command, the configuration of ip http access-class access-list-number will be removed and the configuration of ip http access-class ipv4 access-list-number will be added to the running configuration.

- If ip http access-class access-list-number is already configured and you try to configure using ip http access-class ipv4 access-list-name command, the configuration of ip http access-class access-list-number will be removed and the configuration of ip http access-class ipv4 access-list-name will be added to the running configuration.

- If ip http access-class ipv4 access-list-number is already configured and you try to configure using ip http access-class access-list-name, the configuration of ip http access-class ipv4 access-list-number will be removed from configuration and the configuration of ip http access-class access-list-name will be added to the running configuration.

- If ip http access-class ipv4 access-list-name is already configured and you try to configure using ip http access-class access-list-number, the configuration of ip http access-class ipv4 access-list-name will be removed from configuration and the configuration of ip http access-class access-list-number will be added to the running configuration.

**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 access-class { ipv4 {access-list-number | access-list-name} | ipv6 {access-list-name} }
11. ip http max-connections value
12. ip http timeout-policy idle seconds life seconds requests value
13. 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>
</tbody>
</table>

Switch# show ip http server status |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HTTP secure server capability: Present or HTTP secure server capability: Not present</td>
</tr>
</tbody>
</table>

**Step 2**

**configure terminal**

**Example:**

Switch# configure terminal

Enters global configuration mode.

**Step 3**

**ip http secure-server**

**Example:**

Switch(config)# ip http secure-server

Enables the HTTPS server if it has been disabled. The HTTPS server is enabled by default.

**Step 4**

**ip http secure-port** `port-number`

**Example:**

Switch(config)# ip http secure-port 443

(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.

**Step 5**

**ip http secure-ciphersuite** `{[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}`

**Example:**

Switch(config)# ip http secure-ciphersuite rc4-128-md5

(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.

**Step 6**

**ip http secure-client-auth**

**Example:**

Switch(config)# ip http secure-client-auth

(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.

**Step 7**

**ip http secure-trustpoint** `name`

**Example:**

Switch(config)# ip http secure-trustpoint your_trustpoint

Specifies the CA trustpoint to use to get an X.509v3 security certificate and to authenticate the client certificate connection.

**Note**

Use of this command assumes you have already configured a CA trustpoint according to the previous procedure.
### Configuring the Secure HTTP Client

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP client:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong>&lt;br&gt;ip http path <em>path-name</em>&lt;br&gt;Example:&lt;br&gt;Switch(config)# ip http path /your_server:80</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><strong>Step 9</strong>&lt;br&gt;ip http access-class <em>access-list-number</em>&lt;br&gt;Example:&lt;br&gt;Switch(config)# ip http access-class 2</td>
<td>(Optional) Specifies an access list to use to allow access to the HTTP server.</td>
</tr>
<tr>
<td><strong>Step 10</strong>&lt;br&gt;ip http access-class { ipv4 { access-list-number</td>
<td>access-list-name }</td>
</tr>
<tr>
<td><strong>Step 11</strong>&lt;br&gt;ip http max-connections <em>value</em>&lt;br&gt;Example:&lt;br&gt;Switch(config)# ip http max-connections 4</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>
</tbody>
</table>
| **Step 12**<br>ip http timeout-policy idle *seconds* life *seconds* requests *requests* *value*<br>Example:<br>Switch(config)# ip http timeout-policy idle 120 life 240 requests 1 | (Optional) Specifies how long a connection to the HTTP server can remain open under the defined circumstances:  
  - **idle**—the maximum time period when no data is received or response data cannot be sent. The range is 1 to 600 seconds. The default is 180 seconds (3 minutes).  
  - **life**—the maximum time period from the time that the connection is established. The range is 1 to 86400 seconds (24 hours). The default is 180 seconds.  
  - **requests**—the maximum number of requests processed on a persistent connection. The maximum value is 86400. The default is 1. |
| **Step 13**<br>end<br>Example:<br>Switch(config)# end | Returns to privileged EXEC mode. |
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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** configure terminal  
  Example: Switch# configure terminal | Enters global configuration mode. |
| **Step 2** ip http client secure-trustpoint name  
  Example: Switch(config)# ip http client secure-trustpoint your_trustpoint | (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. |
| **Step 3** ip http client secure-ciphersuite \{[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]\}  
  Example: Switch(config)# ip http client secure-ciphersuite rc4-128-md5 | (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. |
| **Step 4** end  
  Example: Switch(config)# end | Returns to privileged EXEC mode. |

**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>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 hostname hostname</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>Example: Switch(config)# hostname your_hostname</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip domain-name domain-name</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>Example: Switch(config)# ip domain-name your_domain</td>
<td></td>
</tr>
<tr>
<td>Step 4 crypto key generate rsa</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>Example: Switch(config)# crypto key generate rsa</td>
<td></td>
</tr>
<tr>
<td>Step 5 crypto ca trustpoint name</td>
<td>Specifies a local configuration name for the CA trustpoint and enter CA trustpoint configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# crypto ca trustpoint your_trustpoint</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 6</strong> enrollment url <code>url</code></td>
<td>Specifies the URL to which the switch should send certificate requests.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (ca-trustpoint)# enrollment url</td>
<td></td>
</tr>
<tr>
<td><code>http://your_server:80</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> enrollment http-proxy <code>host-name port-number</code></td>
<td>(Optional) Configures the switch to obtain certificates from the CA through an HTTP proxy server.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (ca-trustpoint)# enrollment http-proxy</td>
<td></td>
</tr>
<tr>
<td><code>your_host</code> 49</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> crl query <code>url</code></td>
<td>Configures the switch to request a certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (ca-trustpoint)# crl query</td>
<td></td>
</tr>
<tr>
<td><code>ldap://your_host:49</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> primary <code>name</code></td>
<td>(Optional) Specifies that the trustpoint should be used as the primary (default) trustpoint for CA requests.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (ca-trustpoint)# primary <code>your_trustpoint</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> exit</td>
<td>Exits CA trustpoint configuration mode and return to global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> crypto ca authentication <code>name</code></td>
<td>Authenticates the CA by getting the public key of the CA. Use the same name used in Step 5.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (config)# crypto ca authentication</td>
<td></td>
</tr>
<tr>
<td><code>your_trustpoint</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> crypto ca enroll <code>name</code></td>
<td>Obtains the certificate from the specified CA trustpoint. This command requests a signed certificate for each RSA key pair.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (config)# crypto ca enroll <code>your_trustpoint</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td></td>
</tr>
<tr>
<td>Switch (config)# end</td>
<td></td>
</tr>
</tbody>
</table>
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>
<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 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
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(config)# enrollment url http://example.com
Device(config)#  crl query ldap://example.com
Device(config)#  primary
Device(config)# 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>Cisco IOS Master Command List, All Releases</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 Secure Socket Layer HTTP

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</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 40

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 709
• Prerequisites For Certification Authority, on page 709
• Restrictions for Certification Authority, on page 709
• Information About Certification Authority, on page 710
• How to Configure Certification Authority, on page 711
• Monitoring and Maintaining Certification Authority, on page 718

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.

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 nvram: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:

```
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".

**GENERAL STEPS**

1. `enable`
2. `configure terminal`
3. `hostname name`

**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><strong>Step 1</strong> crypto ca certificate query</td>
<td>Enables query mode, which causes certificates and CRLs not to be stored locally.</td>
</tr>
<tr>
<td>Example: <code>Device(config)# crypto ca certificate query</code></td>
<td></td>
</tr>
</tbody>
</table>

Note: Query mode may affect availability if the CA is down.
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><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> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>hostname name</code></td>
<td>Configures the host name of the device.</td>
</tr>
<tr>
<td>Example: Device(config)# hostname device1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip domain-name name</code></td>
<td>Configures the IP domain name of the device.</td>
</tr>
<tr>
<td>Example: Device(config)# ip domain-name domain.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></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>

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> <code>enable</code></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> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>hostname name</code></td>
<td>Configures the host name of the device.</td>
</tr>
<tr>
<td>Example: Device(config)# hostname device1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip domain-name name</code></td>
<td>Configures the IP domain name of the device.</td>
</tr>
<tr>
<td>Example: Device(config)# ip domain-name domain.com</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></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></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></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# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 3    | crypto ca trustpoint name  
**Example:**  
Device(config)# crypto ca trustpoint ka | Declares the certification authority (CA) that your device should use and enters the CA profile enroll configuration mode. |
| 4    | enrollment url url  
**Example:**  
Device(ca-profile-enroll)# enrollment url http://entrust:81 | Specifies the URL of the CA server to which enrollment requests are sent. |
| 5    | enrollment command  
**Example:**  
Device(ca-profile-enroll)# enrollment command | Specifies the HTTP command that is sent to the CA for enrollment. |
| 6    | exit  
**Example:**  
Device(ca-profile-enroll)# exit | Exit CA profile enroll configuration mode and returns to global configuration mode. |
| 7    | crypto pki trustpoint name  
**Example:**  
Device(config)# crypto pki trustpoint ka | Declares the trustpoint that your device should use and enters Ca-trustpoint configuration mode. |
| 8    | crl query ldap://url:[port]  
**Example:**  
Device(ca-trustpoint)# crl query ldap://bar.cisco.com:3899 | Queries the certificate revocation list (CRL) to ensure that the certificate of the peer is not revoked. |
| 9    | enrollment {mode ra | retry count number | retry period minutes | url url}  
**Example:**  
Device(ca-trustpoint)# enrollment retry period 2 | Specifies the enrollment wait period between certificate request retries. |
| 10   | enrollment {mode ra | retry count number | retry period minutes | url url}  
**Example:**  
Device(ca-trustpoint)# enrollment retry count 8 | Specifies the number of times a device will resend a certificate request when it does not receive a response from the previous request. |
| 11   | revocation-check method1 [method2 method3]  
**Example:**  
Device(ca-trustpoint)# revocation-check crl ocsp | Checks the revocation status of a certificate. |
| 12   | end  
**Example:**  
Device(ca-trustpoint)# end | Exit CA trustpoint configuration mode and returns to privileged EXEC mode. |
## 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> 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 name</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 ca trustpoint ka</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> revocation-check method1 [method2 method3]</td>
<td>Checks the revocation status of a certificate.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-trustpoint)# revocation-check ocsp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> root tftp server-hostname filename</td>
<td>Obtains the certification authority (CA) certificate via TFTP.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-trustpoint)# root tftp server1 file1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> enrollment http-proxy hostname port-number</td>
<td>Accesses the certification authority (CA) by HTTP through the proxy server.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-trustpoint)# enrollment http-proxy host2 8080</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Exits CA trustpoint configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(ca-trustpoint)# end</td>
<td></td>
</tr>
</tbody>
</table>
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*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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> 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> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki authenticate<em>name</em></td>
<td>Authentiﬁes the CA by getting the certificate of the CA.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# crypto pki authenticate myca</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits global conﬁguration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> 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> Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki enroll number</td>
<td>Obtains certificates for your device from the CA.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# crypto pki enroll myca</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

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> 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 pki crl request name</td>
<td>Requests that a new certificate revocation list (CRL) be obtained immediately from the CA.</td>
</tr>
<tr>
<td>Example: Device(config)# crypto pki crl request myca</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**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><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Device&gt; 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: <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>crypto pki trustpoint name</code></td>
<td>Declares the trustpoint that your device should use and enters CA trustpoint configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Device(ca-trustpoint)# crypto pki trustpoint mytp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>crl query ldap://url:[port]</code></td>
<td>Queries the CRL to ensure that the certificate of the peer has not been revoked.</td>
</tr>
<tr>
<td>Example: <code>Device(ca-trustpoint)# crl query ldap://url:[port]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>Exits CA trustpoint configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Device(ca-trustpoint)# end</code></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>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>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Deletes all Rivest, Shamir, and Adelman (RSA) keys from your device.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>crypto key zeroize rsa</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></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>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>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>- Enter your password if prompted.</td>
</tr>
</tbody>
</table>
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>
<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>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 2</strong> show crypto pki certificates</td>
<td>Displays information about your device certificate, the certification authority (CA) certificate, and any registration authority (RA) certificates.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# show crypto pki certificates</td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 4</strong> crypto pki certificate chain name</td>
<td>Enters certificate chain configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# crypto pki certificate chain myca</td>
</tr>
<tr>
<td><strong>Step 5</strong> no certificate certificate-serial-number</td>
<td>Deletes the certificate.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits certificate chain configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-cert-chain)# exit</td>
</tr>
<tr>
<td><strong>Step 7</strong> no crypto pki import name certificate</td>
<td>Deletes a certificate manually.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# no crypto pki import MS certificate</td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# exit</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></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&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>show crypto key mypubkey rsa [keyname]</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show crypto key mypubkey rsa [keyname]</td>
</tr>
<tr>
<td></td>
<td>Displays the RSA public keys configured on a device.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show crypto key pubkey-chain rsa</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show crypto key pubkey-chain rsa</td>
</tr>
<tr>
<td></td>
<td>Displays the RSA public keys of the peer that are stored on a device.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show crypto key pubkey-chain rsa [name key-name</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show crypto key pubkey-chain rsa address 209.165.202.129</td>
</tr>
<tr>
<td></td>
<td>Displays the address of a specific key.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show crypto pki certificates</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show crypto pki certificates</td>
</tr>
<tr>
<td></td>
<td>Displays information about the device certificate, the certification authority (CA) certificate, and any registration authority (RA) certificates</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show crypto pki trustpoints</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# show crypto pki certificates</td>
</tr>
<tr>
<td></td>
<td>Displays trustpoints that are configured on a device.</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, on page 725
- Information About Access Control Lists, on page 725

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 (vty), 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 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.

```
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 84: 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 172.18.0.0</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>172.18.8.0/29</td>
<td>0.0.0.7</td>
<td>Only subnet 172.18.8.0/29 matches</td>
</tr>
<tr>
<td>172.18.8.8/29</td>
<td>0.0.0.7</td>
<td>Only subnet 172.18.8.8/29 matches</td>
</tr>
<tr>
<td>172.18.8.15/30</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 the following type of ACL to filter traffic:

- Port ACLs access-control traffic entering a Layer 2 interface. You can apply port ACLs to a Layer 2 interface in each input direction to each access list type — IPv4 and MAC.

**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 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 56: 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.
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.

  **Note**

  For TCP ACEs with L4 Ops, the fragmented packets will be dropped per RFC 1858.

- 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.
CHAPTER 42

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 735
- Restrictions for Configuring IPv4 Access Control Lists, on page 735
- Information About Configuring IPv4 Access Control Lists, on page 736
- How to Configure ACLs, on page 744
- Monitoring IPv4 ACLs, on page 761
- Configuration Examples for ACLs, on page 761
- Examples: Troubleshooting ACLs, on page 767
- Additional References, on page 768
- Feature Information for IPv4 Access Control Lists, on page 769

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.

• 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 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 lists 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 85: 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.

**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.

**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 affect 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**

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.

---

**Note**

Access lists that are applied to interfaces on a device do not filter traffic that originates from that device.

---

**Figure 57: 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.

---

**Note**

The behavior described above applies to all single-CPU platforms that run Cisco software.

---

**ACL Logging**

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**

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

Follow the procedure given below 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.

**DETAILED STEPS**

**Step 1** Create an ACL by specifying an access list number or name and the access conditions.

**Step 2** Apply the ACL to interfaces.

### 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:</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> access-list access-list-number {deny</td>
<td>permit} source source-wildcard [log]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# access-list 2 deny your_host</td>
<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>
</tr>
<tr>
<td></td>
<td>The source is the source address of the network or host from which the packet is being sent specified as:</td>
</tr>
<tr>
<td></td>
<td>• The 32-bit quantity in dotted-decimal format.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>• The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0.</td>
</tr>
<tr>
<td></td>
<td>(Optional) The source-wildcard applies wildcard bits to the source.</td>
</tr>
<tr>
<td></td>
<td>(Optional) Enter log to cause an informational logging message about the packet that matches the entry to be sent to the console.</td>
</tr>
<tr>
<td></td>
<td>Note Logging is supported only on ACLs attached to Layer 3 interfaces.</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>
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] [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] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]`
4. `access-list access-list-number {deny | permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [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] [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><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Verifies your entries.

((Optional) Saves your entries in the configuration file.)

**Example:**

Switch# show running-config

Switch# copy running-config startup-config
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Defines an extended IPv4 access list and the access conditions.</td>
</tr>
</tbody>
</table>

### Step 2

**access-list access-list-number \{deny | permit\} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]**

**Example:**

Switch(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log

---

**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).

- **fragments**—Enter to check non-initial fragments.

- **tos**—Enter to match by type of service level, specified by a number from 0 to 15 or a name: normal (0),...
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-reliability (2), max-throughput (4), min-delay (8).</td>
</tr>
<tr>
<td>• <strong>time-range</strong>—Specify the time-range name.</td>
</tr>
<tr>
<td>• <strong>dscp</strong>—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>
</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

**access-list** `access-list-number` {deny | permit} tcp `source source-wildcard` [operator port] `destination destination-wildcard` [operator port] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] [flag]

**Example:**

```
Switch(config)# access-list 101 permit tcp any any eq 500
```

This 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:

- **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

**access-list** `access-list-number` {deny | permit} udp `source source-wildcard` [operator port] `destination destination-wildcard` [operator port] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]

**Example:**

```
Switch(config)# access-list 101 permit udp any any eq 100
```

(Optional) Defines an extended UDP access list and the access conditions.

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 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]

**Example:**

```
Switch(config)# access-list 101 permit icmp any any
```

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
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| precedence [tos tos] [fragments] [time-range time-range-name] [dscp dscp] | 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. |

**Example:**

Switch(config)# access-list 101 permit icmp any any 200

---

**Step 6**

- access-list access-list-number {deny | permit} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] 
- **Example:**
  
  Switch(config)# access-list 101 permit igmp any any 14

(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**

- **Example:**

  Switch(config)# end

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>
</table>
| **Step 1**  
<code>enable</code>  
**Example:**  
<code>Switch> enable</code> | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2**  
<code>configure terminal</code>  
**Example:**  
<code>Switch# configure terminal</code> | Enters global configuration mode. |
| **Step 3**  
<code>ip access-list standard name</code>  
**Example:**  
<code>Switch(config)# ip access-list standard 20</code> | 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. |
| **Step 4**  
Use one of the following:  
• <code>deny {source [source-wildcard] | host source | any} [log]</code>  
• <code>permit {source [source-wildcard] | host source | any} [log]</code>  
**Example:**  
<code>Switch(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</code>  
<code>or</code>  
<code>Switch(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</code> | In access-list configuration mode, specify one or more conditions denied or permitted to decide if the packet is forwarded or dropped.  
• <code>host source</code>—A source and source wildcard of source 0.0.0.0.  
• <code>any</code>—A source and source wildcard of 0.0.0.0 255.255.255.255. |
| **Step 5**  
<code>end</code>  
**Example:**  
<code>Switch(config-std-nacl)# end</code> | Returns to privileged EXEC mode. |
| **Step 6**  
<code>show running-config</code>  
**Example:**  
<code>Switch# show running-config</code> | Verifies your entries. |
Creating Extended Named ACLs

Follow the procedure given below 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] [log] [time-range time-range-name]`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

**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. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch&gt; enable</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>Switch# configure terminal</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>ip access-list extended name</td>
<td>Defines an extended IPv4 access list using a name, and enter access-list configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Switch(config)# ip access-list extended 150</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>{deny</td>
<td>permit} protocol [source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• host source—A source and source wildcard of source 0.0.0.0.</td>
</tr>
</tbody>
</table>
Sequencing Access-List Entries and Revising the Access List

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config-ext-nacl)# permit 0 any any | - 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**

Example:

Switch(config-ext-nacl)# end

Returns to privileged EXEC mode.

**Step 6**

Example:

Switch# show running-config

Verifies your entries.

**Step 7**

Example:

Switch# copy running-config startup-config

(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.

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>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> 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>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Sequencing Access-List Entries and Revising the Access List

**Command or Action**

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP access list by name and enters named access list configuration mode.</td>
<td>Device(config)# ip access-list resequence kmd1 100 15</td>
</tr>
</tbody>
</table>

**Step 4**

- **ip access-list {standard|extended} access-list-name**

  **Example:**
  
  Device(config)# ip access-list standard kmd1

- **Step 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]`

  **Example:**
  
  Device(config-std-nacl)# 105 permit 10.5.5.5 0.0.0.0 255

- **Step 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]`

  **Example:**
  
  Device(config-std-nacl)# 105 deny 10.6.6.7 0.0.0.0 255

- **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

**Specifications:**

- **Step 4**

  - If you specify `standard`, make sure you subsequently specify `permit` and/or `deny` statements using the standard access list syntax.
  
  - If you specify `extended`, make sure you subsequently specify `permit` and/or `deny` statements using the extended access list syntax.

- **Step 5**

  - This access list happens to use a `permit` statement first, but a `deny` statement could appear first, depending on the order of statements you need.
  
  - As the prompt indicates, this access list was a standard access list. If you had specified `extended` in Step 4, the prompt for this step would be Device(config-ext-nacl) and you would use the extended `permit` command syntax.

- **Step 6**

  - This access list uses a `permit` statement first, but a `deny` statement could appear first, depending on the order of statements you need.
  
  - As the prompt indicates, this access list was a standard access list. If you had specified `extended` in Step 4, the prompt for this step would be Device(config-ext-nacl) and you would use the extended `deny` command syntax.

- **Step 7**

  - This access list happens to use a `permit` statement first, but a `deny` statement could appear first, depending on the order of statements you need.
  
  - See the `permit (IP)` command for additional command syntax to permit upper layer protocols (ICMP, IGMP, TCP, and UDP).
  
  - Use the `no sequence-number` command to delete an entry.
### Command or Action

**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

**Purpose**

(Optional) Specifies a deny statement in named IP access list mode.

- This access list happens to use a `permit` statement first, but a `deny` statement could appear first, depending on the order of statements you need.
- See the deny (IP) command for additional command syntax to permit upper layer protocols (ICMP, IGMP, TCP, and UDP).
- Use the `no sequence-number` command to delete an entry.

**Step 9**

Repeat Step 5 and/or Step 6 to add sequence number statements, as applicable.

**Example:**

Device(config-ext-nacl)# 150 deny tcp any any log

**Purpose**

Allows you to revise the access list.

**Step 10**

`end`

**Example:**

Device(config-ext-nacl)# end

**Purpose**

(Optional) Exits the configuration mode and returns to privileged EXEC mode.

**Step 11**

`show ip access-lists access-list-name`

**Example:**

Device# show ip access-lists kmd1

**Purpose**

(Optional) Displays the contents of the IP access list.

### 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

```
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>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>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Identifies the access list by a name or number and enters extended named access list configuration mode.</td>
</tr>
<tr>
<td>`ip access-list {standard</td>
<td>extended} {name</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Adds a remark for an entry in a named IP access list.</td>
</tr>
<tr>
<td><code>remark remark</code></td>
<td>• The remark indicates the purpose of the <code>permit</code> or <code>deny</code> statement.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ext-nacl)# remark Do not allow host1 subnet to telnet out</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Sets conditions in a named IP access list that denies packets.</td>
</tr>
<tr>
<td><code>deny protocol host host-address any eq port</code></td>
<td>Device(config-ext-nacl)# deny tcp host 172.16.2.88 any eq telnet</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits extended named access list configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Device(config-ext-nacl)# end</td>
</tr>
</tbody>
</table>

**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]`
### Configuring Time Ranges for ACLs

- **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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# 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>Assigns a meaningful name (for example, <code>workhours</code>) 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><code>time-range time-range-name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# time-range workhours</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies when the function it will be applied to is operational.</td>
</tr>
<tr>
<td>Use one of the following:</td>
<td></td>
</tr>
<tr>
<td>• <strong>absolute</strong> <code>[start time date] [end time date]</code></td>
<td></td>
</tr>
<tr>
<td>• <strong>periodic</strong> <code>day-of-the-week hh:mm to [day-of-the-week] hh:mm</code></td>
<td></td>
</tr>
<tr>
<td>• <strong>periodic</strong> `{weekdays</td>
<td>weekend</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006</code></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config-time-range)# periodic weekdays 8:00 to 12:00</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</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>
</tbody>
</table>

---

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
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}
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><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>`line [console</td>
<td>vty] line-number`</td>
</tr>
<tr>
<td><code>access-class access-list-number {in}</code></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</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 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>Step 3</td>
<td>line [console</td>
<td>vty] line-number</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# line console 0</td>
<td>• console—Specifies the console terminal line. The console port is DCE.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• vty—Specifies a virtual terminal for remote console access.</td>
</tr>
<tr>
<td></td>
<td></td>
<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>
</tr>
<tr>
<td>Step 4</td>
<td>access-class access-list-number {in}</td>
<td>Restricts incoming connections between a particular virtual terminal line (into a device) and the addresses in an access list.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-line)# access-class 10 in</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-line)# end</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# show running-config</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### 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
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> 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>Identifies a specific interface for configuration, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/1</td>
<td>The interface can be a Layer 2 interface (port ACL).</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip access-group {access-list-number</td>
<td>name} in</td>
</tr>
<tr>
<td>Example: Switch(config-if)# ip access-group 2 in</td>
<td></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>
<tr>
<td><strong>Step 5</strong> show running-config</td>
<td>Displays the access list configuration.</td>
</tr>
<tr>
<td>Example: 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: 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.

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>
<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>
<tr>
<td><code>show mac access-group [interface interface-id]</code></td>
<td>Displays MAC access lists applied to all Layer 2 interfaces or the specified Layer 2 interface.</td>
</tr>
</tbody>
</table>

Configuration Examples for ACLs

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
```
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 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, 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. Because the secure system of the network always accepts mail connections on port 25, the incoming are separately controlled.

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 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)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit

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 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
  70 permit ip host 10.3.3.3 any log
  80 permit tcp host 10.3.3.3 host 10.1.2.2
  90 permit ip host 10.3.3.3 any
  100 permit ip any any

Router(config)# ip access-list extended carls
Router(config)# ip access-list resequence carls 1 2
Router(config)# end
```

```
Router# show access-list carls
Extended IP access list carls
  1 permit ip host 10.3.3.3 host 172.16.5.34
  3 permit icmp any any
  5 permit tcp any host 10.3.3.3
  7 permit ip host 10.4.4.4 any
  9 Dynamic test permit ip any any
  11 permit ip host 172.16.2.2 host 10.3.3.12
  13 permit ip host 10.3.3.3 any log
  15 permit tcp host 10.3.3.3 host 10.1.2.2
  17 permit ip host 10.3.3.3 any
  19 permit ip any any
```
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(config)# 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
Router(config-std-nacl)# end
Router(config)# 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
  40 permit 10.4.4.4, wildcard bits 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
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
Switch(config-if)# ip access-group strict in
```

Examples: ACL Logging

Two variations of logging are supported on 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
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
```
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.

```conffile
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-ext-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-IPACCESSLOGP` 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
```

### 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.

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:

```
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:

```
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 the 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 for IPv4 Access Control Lists

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>IPv4 Access Control Lists perform packet filtering to control which packets move</td>
</tr>
<tr>
<td></td>
<td>through the network and where. Such control provides security by helping to</td>
</tr>
<tr>
<td></td>
<td>limit network traffic, restrict the access of users and devices to the network,</td>
</tr>
<tr>
<td></td>
<td>and prevent traffic from leaving a network. This feature was introduced.</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</td>
</tr>
<tr>
<td></td>
<td>allows you to specify noncontiguous ports in a single access control entry, which</td>
</tr>
<tr>
<td></td>
<td>greatly reduces the number of entries required in an access control list when</td>
</tr>
<tr>
<td></td>
<td>several entries have the same source address, destination address, and protocol,</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>numbers to permit or deny statements and also reorder, add, or remove such</td>
</tr>
<tr>
<td></td>
<td>statements from a named IP access list. This feature makes revising IP access</td>
</tr>
<tr>
<td></td>
<td>lists much easier. Prior to this feature, users could add access list entries to</td>
</tr>
<tr>
<td></td>
<td>the end of an access list only; therefore needing to add statements anywhere except</td>
</tr>
<tr>
<td></td>
<td>the end required reconfiguring the access list entirely.</td>
</tr>
<tr>
<td></td>
<td>The following commands were introduced or modified: deny (IP), ip access-list</td>
</tr>
<tr>
<td></td>
<td>resequence deny (IP), permit (IP).</td>
</tr>
</tbody>
</table>
CHAPTER 43

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 771
• Restrictions for IPv6 ACLs, on page 771
• Information About Configuring IPv6 ACLs, on page 772
• How to Configure IPv6 ACLs, on page 774
• Configuration Examples for IPv6 ACLs, on page 782
• Additional References, on page 783
• Feature Information for IPv6 Access Control Lists, on page 784

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: routing header, and undetermined-transport.
• The switch does not support reflexive ACLs (the `reflect` keyword).

• This release does not support router ACL and VLAN ACLs (VLAN maps) for IPv6.

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

• 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.

IPv6 ACLs on the switch have these characteristics:

• Fragmented frames (the `fragments` keyword as in IPv6) are not supported.

• 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 processed to the CPU, and the ACLs are 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 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.

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 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, the packets associated with the ACL are processed to the CPU, and the ACLs are applied in software.

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.

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} [operator [port-number]] {destination-ipv6-prefix/prefix-length|any} [operator [port-number]] [dscp value] [fragments] [log] [log-input] [sequence value] [time-range name]`
5. `{deny | permit} tcp {source-ipv6-prefix/prefix-length|any} [operator [port-number]] {destination-ipv6-prefix/prefix-length|any} [operator [port-number]] [ack] [dscp value] [fin] [log] [log-input] [neq {port|protocol}] [psh] [range {port|protocol}] [rst] [sequence value] [syn] [time-range name] [urg]`
6. `{deny | permit} udp {source-ipv6-prefix/prefix-length|any} [operator [port-number]] {destination-ipv6-prefix/prefix-length|any} [operator [port-number]] [dscp value] [log] [log-input] [neq {port|protocol}] [range {port|protocol}] [sequence value] [time-range name]`
7. `{deny | permit} icmp {source-ipv6-prefix/prefix-length|any} [operator [port-number]] {destination-ipv6-prefix/prefix-length|any} [operator [port-number]] [icmp-type [icmp-code] | icmp-message] [dscp value] [log] [log-input] [sequence value] [time-range name]`
8. `end`
9. `show ipv6 access-list`
10. show running-config
11. 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.  
\> Enter your password if prompted. |
| Step 2 | configure terminal | Enters global configuration mode. |
| Step 3 | ipv6 access-list list-name | Defines an IPv6 ACL name, and enters IPv6 access list configuration mode. |
| Step 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][sequence value] [time-range name] | Enter deny or permit to specify whether to deny or permit the packet if conditions are matched. These are the conditions:  
- 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.  
- 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. |
### Purpose

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.

- (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.

- (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.

- (Optional) Enter **fragments** to check noninitial fragments. This keyword is visible only if the protocol is ipv6.

- (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.

- (Optional) Enter **sequence value** to specify the sequence number for the access list statement. The acceptable range is from 1 to 4,294,967,295.

- (Optional) Enter **time-range name** to specify the time range that applies to the deny or permit statement.

### 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] [fin] [log] [log-input] [neq {port | protocol}] [psh] [range {port | protocol}] [rst] [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.
- **fin**—Finished bit set; no more data from sender.
- **neq** `{port | protocol}`—Matches only packets that are not on a given port number.
- **psh**—Push function bit set.
- **range** `{port | protocol}`—Matches only packets in the port number range.
- **rst**—Reset bit set.
- **syn**—Synchronize bit set.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>• <strong>urg</strong>—Urgent pointer bit set.</td>
</tr>
</tbody>
</table>

```
{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}] [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.

```
{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] [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 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
end
```

Return to privileged EXEC mode.

```
Step 9
show ipv6 access-list
```

Verify the access list configuration.

```
Step 10
show running-config
```

Verifies your entries.

```
Switch# show running-config
```

```
Step 11
copy running-config startup-config
```

(Optional) Saves your entries in the configuration file.

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

What to do next

Attach the IPv6 ACL to an Interface
# Attaching an IPv6 ACL to an Interface

You can apply an ACL to inbound traffic on Layer 2 interfaces. Follow these steps to control access to an interface:

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `ipv6 address ipv6-address`
5. `ipv6 traffic-filter access-list-name in`
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>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>Identify a Layer 2 interface on which to apply an access list, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 address ipv6-address</td>
<td>This command is not required on Layer 2 interfaces or if the interface has already been configured with an explicit IPv6 address.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ipv6 traffic-filter access-list-name in</td>
<td>Apply the access list to incoming traffic on the interface.</td>
</tr>
<tr>
<td>Note</td>
<td>The <code>out</code> keyword is not supported for Layer 2 interfaces (port ACLs).</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
### Step 7

**show running-config**  
**Example:**  
```
Switch# show running-config
```

**Purpose:** 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.

---

### 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>show access-lists</td>
<td>Displays all access lists configured on the switch.</td>
</tr>
<tr>
<td>show ipv6 access-list [access-list-name]</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.

```
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-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
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>
</tbody>
</table>

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

| Step 3 | ipv6 access-list access-list-name | Defines an IPv6 ACL and enters IPv6 access list configuration mode. |
| **Example:** Device(config)# ipv6 access-list list1 | |

| Step 4 | exit | Exits IPv6 access list configuration mode and enters global configuration mode. |
| **Example:** Device(config-ip6-acl)# exit | |

| Step 5 | interface type number | Specifies an interface type and number and enters interface configuration mode. |
| **Example:** Device(config)# interface Gigabitethernet 0/1 | |

| Step 6 | ipv6 traffic-filter access-list-name in | Filters incoming IPv6 traffic on an interface. |
| **Example:** Device(config-if)# ipv6 traffic-filter list1 in | |
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step 7</th>
<th>end</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-if)# end</td>
<td>Exits interface configuration mode and enters privileged EXEC mode.</td>
</tr>
</tbody>
</table>

## 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} [operator [port-number]] {destination-ipv6-prefix|prefix-length | any | host destination-ipv6-address} [operator [port-number]] [dscp value] [hhb] [log] [log-input] [reflect name [timeout value]] [sequence value] [time-range 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>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>* Enter your password if prompted.</td>
<td></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>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ipv6 access-list <em>access-list-name</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ipv6 access-list hbh-acl</td>
</tr>
<tr>
<td>Defines an IPv6 ACL and enters IPv6 access list configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>permit protocol `{source-ipv6-prefix</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config-ipv6-acl)# permit icmp any any dest-option-type</td>
</tr>
<tr>
<td>Sets permit conditions for the IPv6 ACL.</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

```plaintext
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

```plaintext
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

```plaintext
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)# exit
```

! Assign an IP address and add the ACL on the interface.

```plaintext
Device(config)# interface gigabitethernet0/1
```

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** | **Example:**
| `Device(config-ipv6-acl)# deny icmp any any dest-option-type` | Sets deny conditions for the IPv6 ACL. |
| **Step 6** | **Example:**
| `Device (config-ipv6-acl)# end` | Returns to privileged EXEC configuration mode. |
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 "show interface" counters on all interfaces [confirm]
Device#

! Verify the configurations.

Device# show running-config interface gigabitethernet0/1

Building configuration...

Current configuration : 114 bytes
!
interface gigabitethernet0/1
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 the 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:</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 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 87: 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>Cisco IOS Release 15.2(5)E</td>
<td>Allows you to control IPv6 traffic that might contain hop-by-hop extension headers. The following commands were introduced or modified: <code>deny (IPv6)</code>, <code>permit (IPv6)</code>.</td>
</tr>
<tr>
<td>IPv6 PACL Support</td>
<td>Cisco IOS Release 15.2(5)E</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. The following command was introduced or modified: <code>ipv6 traffic-filter</code>.</td>
</tr>
<tr>
<td>IPv6 Services: Extended Access Control Lists</td>
<td>Cisco IOS Release 15.2(5)E</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>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6 Services: Standard Access Control Lists</td>
<td>Cisco IOS Release 15.2(5)E</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 787
- Information About DHCP, on page 787
- How to Configure DHCP Features, on page 794
- Configuring DHCP Server Port-Based Address Allocation, on page 803

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.

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.

When configuring DHCP snooping to block unauthorized IP address using the `ip verify source prot-security` command on an interface, the `switchport port-security` command should also be configured.

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 DHCP OFFER, DHCPACK, DHCPNAK, or DHCP PLEASEQUERY 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 DHCP RELEASE or DHCP DECLINE 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 798

**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.
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, \textit{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, \textit{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 Ethernet 1/0/25, 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.

Figure 59: Suboption Packet Formats

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:

```xml
<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>
<tbody>
<tr>
<td>DHCP server</td>
<td>Enabled in Cisco IOS software, requires configuration(^8)</td>
</tr>
<tr>
<td>DHCP relay agent</td>
<td>Enabled(^2)</td>
</tr>
<tr>
<td>DHCP packet forwarding address</td>
<td>None configured</td>
</tr>
<tr>
<td>Checking the relay agent information</td>
<td>Enabled (invalid messages are dropped)</td>
</tr>
<tr>
<td>DHCP relay agent forwarding policy</td>
<td>Replace the existing relay agent information</td>
</tr>
<tr>
<td>DHCP snooping enabled globally</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping information option</td>
<td>Enabled</td>
</tr>
<tr>
<td>DHCP snooping option to accept packets on untrusted input interfaces(^9)</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping limit rate</td>
<td>None configured</td>
</tr>
<tr>
<td>DHCP snooping trust</td>
<td>Untrusted</td>
</tr>
<tr>
<td>DHCP snooping VLAN</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP snooping MAC address verification</td>
<td>Enabled</td>
</tr>
<tr>
<td>Cisco IOS DHCP server binding database</td>
<td>Enabled in Cisco IOS software, requires configuration.</td>
</tr>
<tr>
<td>Note</td>
<td>The switch gets network addresses and configuration parameters only from a device configured as a DHCP server.</td>
</tr>
<tr>
<td>DHCP snooping binding database agent</td>
<td>Enabled in Cisco IOS software, requires configuration.</td>
</tr>
<tr>
<td></td>
<td>This feature is operational only when a destination is configured.</td>
</tr>
</tbody>
</table>

\(^8\) 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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch&gt;</code> <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><strong>Example:</strong> <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> service dhcp</td>
<td>Enables the DHCP server and relay agent on your switch.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>By default, this feature is enabled.</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:
   - interface range port-range
   - interface interface-id

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# service dhcp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></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>Verifies your entries.</td>
</tr>
<tr>
<td>show running-config</td>
<td></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></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></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

- Checking (validating) the relay agent information
- Configuring the relay agent forwarding policy
8. switchport mode access
9. switchport access vlan vlan-id
10. end
11. show running-config
12. copy running-config startup-config

## 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 | |
| 3    | interface vlan vlan-id | Creates a switch virtual interface by entering a VLAN ID, and enter interface configuration mode. |
|      | Example:          |         |
|      | Switch(config)# interface vlan 1 | |
| 4    | ip address ip-address subnet-mask | Configures the interface with an IP address and an IP subnet. |
|      | Example:          |         |
|      | Switch(config-if)# ip address 192.108.1.27 255.255.255.0 | |
| 5    | ip helper-address address | Specifies the DHCP packet forwarding address.  
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. |
|      | Example:          |         |
|      | Switch(config-if)# ip helper-address 172.16.1.2 | |
| 6    | end               | Returns to global configuration mode. |
|      | Example:          |         |
|      | Switch(config-if)# end | |
| 7    | Use one of the following:  
|      | • interface range port-range  
|      | • interface interface-id | Configures multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. |
### Command or Action

<table>
<thead>
<tr>
<th>Example:</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config)# interface gigabitethernet0/2</td>
<td>Configures a single physical port that is connected to the DHCP client, and enter interface configuration mode.</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 788

### 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
### Enabling DHCP Snooping and Option 82

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:</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 dhcp snooping</td>
<td>Enables DHCP snooping globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip dhcp snooping vlan vlan-range</td>
<td>Enables DHCP snooping on a VLAN or range of VLANs. The range is 1 to</td>
</tr>
<tr>
<td>Example:</td>
<td>4094. You can enter a single VLAN ID identified by VLAN ID number, a</td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping vlan 10</td>
<td>series of VLAN IDs separated by commas, a range of VLAN IDs separated</td>
</tr>
<tr>
<td></td>
<td>by hyphens, or a range of VLAN IDs separated by entering the starting</td>
</tr>
<tr>
<td></td>
<td>and ending VLAN IDs separated by a space.</td>
</tr>
<tr>
<td></td>
<td>• You can enter a single VLAN ID identified by VLAN ID number, a series</td>
</tr>
<tr>
<td></td>
<td>of VLAN IDs separated by commas, a range of VLAN IDs separated by</td>
</tr>
<tr>
<td></td>
<td>hyphens, or a range of VLAN IDs separated by entering the starting and</td>
</tr>
<tr>
<td></td>
<td>ending VLAN IDs separated by a space.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip dhcp snooping information option</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>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip dhcp snooping information option</td>
<td></td>
</tr>
</tbody>
</table>
| Step 6 | `ip dhcp snooping information option format remote-id [string ASCII-string | hostname]` | (Optional) Configures the remote-ID suboption. You can configure the remote ID as:
- String of up to 63 ASCII characters (no spaces)
- Configured hostname for the switch

**Note** If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration.

The default remote ID is the switch MAC address.

**Example:**
```
Switch(config)# ip dhcp snooping information option format remote-id string asciistring2
```

| Step 7 | `ip dhcp snooping information option allow-untrusted` | (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.

The default setting is disabled.

**Note** Enter this command only on aggregation switches that are connected to trusted devices.

**Example:**
```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

| Step 8 | `interface interface-id` | Specifies the interface to be configured, and enter interface configuration mode.

**Example:**
```
Switch(config)# interface gigabitethernet 0/1
```

| Step 9 | `ip dhcp snooping vlan vlan information option format-type circuit-id [override] string ASCII-string` | (Optional) Configures the circuit-ID suboption for the specified interface.

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 `vlan-mod-port`.

You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces).

(Optional) Use the `override` keyword when you do not want the circuit-ID suboption inserted in TLV format to define subscriber information.

**Example:**
```
Switch(config-if)# ip dhcp snooping vlan 1 information option format-type curcuit-id override string override2
```

| Step 10 | `ip dhcp snooping trust` | (Optional) Configures the interface as trusted or untrusted. Use the `no` keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.

**Example:**
```
Switch(config-if)# ip dhcp snooping trust
```

| Step 11 | `ip dhcp snooping limit rate rate` | (Optional) Configures the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured.

**Example:**
```
Switch(config-if)# ip dhcp snooping limit rate 100
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one VLAN with DHCP snooping.</td>
</tr>
</tbody>
</table>

**Step 12**

exit

*Example:*

Switch(config-if)# exit

Returns to global configuration mode.

**Step 13**

ip dhcp snooping verify mac-address

*Example:*

Switch(config)# ip dhcp snooping verify mac-address

(Optional) Configures the switch to verify that the source MAC address in a DHCP packet received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.

**Step 14**

decide

*Example:*

Switch(config)# end

Returns to privileged EXEC mode.

**Step 15**

show running-config

*Example:*

Switch# show running-config

Verifies your entries.

**Step 16**

copy running-config startup-config

*Example:*

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

---

### 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 89: Commands for Displaying DHCP Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip dhcp snooping</td>
<td>Displays the DHCP snooping configuration for a switch</td>
</tr>
<tr>
<td>show ip dhcp snooping binding</td>
<td>Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.</td>
</tr>
<tr>
<td>show ip dhcp snooping database</td>
<td>Displays the DHCP snooping binding database status and statistics.</td>
</tr>
<tr>
<td>show ip dhcp snooping statistics</td>
<td>Displays the DHCP snooping statistics in summary or detail form.</td>
</tr>
<tr>
<td>show ip source binding</td>
<td>Display the dynamically and statically configured bindings.</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

#### 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[@]@]hostname | 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><strong>Step 1</strong>&lt;br&gt;<code>enable</code>&lt;br&gt;<code>Example:</code>&lt;br&gt;Switch&gt; <code>enable</code></td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;<code>configure terminal</code>&lt;br&gt;<code>Example:</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Switch# configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip dhcp snooping database {flash[number]:filename</td>
</tr>
<tr>
<td></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>• flash[number]:filename</td>
</tr>
<tr>
<td></td>
<td>• ftp://user:password@host/filename</td>
</tr>
<tr>
<td></td>
<td>• http://[[username:password[@]]/hostname</td>
</tr>
<tr>
<td></td>
<td>• rcp://user@host/filename</td>
</tr>
<tr>
<td></td>
<td>• tftp://host/filename</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip dhcp snooping database timeout seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip dhcp snooping database timeout 300</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip dhcp snooping database write-delay seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip dhcp snooping database write-delay 15</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show ip dhcp snooping database [detail]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show ip dhcp snooping database detail</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# show running-config</td>
</tr>
<tr>
<td></td>
<td>Verifies your entries.</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>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><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><strong>Example:</strong></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></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>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# ip dhcp use subscriber-id client-id</code></td>
<td></td>
</tr>
</tbody>
</table>
**Command or Action** | **Purpose**
--- | ---
**Step 4**  
`ip dhcp subscriber-id interface-name`  
Example:  
Switch(config)# `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.

**Step 5**  
`interface interface-id`  
Example:  
Switch(config)# `interface gigabitethernet`  `0/1`  
Specifies the interface to be configured, and enter interface configuration mode.

**Step 6**  
`ip dhcp server use subscriber-id client-id`  
Example:  
Switch(config-if)# `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.

**Step 7**  
`end`  
Example:  
Switch(config)# `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.

---

**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 90: Commands for Displaying DHCP Port-Based Address Allocation Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interface interface id</code></td>
<td>Displays the status and configuration of a specific interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------</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 the 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 DHCP Snooping and Option 82

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release</td>
<td>Feature Information</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>Introduced support for the following commands:</td>
</tr>
<tr>
<td></td>
<td>• <strong>show ip dhcp snooping statistics</strong> user EXEC command for displaying DHCP snooping statistics.</td>
</tr>
<tr>
<td></td>
<td>• <strong>clear ip dhcp snooping statistics</strong> privileged EXEC command for clearing the snooping statistics counters.</td>
</tr>
</tbody>
</table>
CHAPTER 45

Configuring IP Source Guard

- Finding Feature Information, on page 811
- Information About IP Source Guard, on page 811
- How to Configure IP Source Guard, on page 813
- Monitoring IP Source Guard, on page 816
- Additional References, on page 817

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 IP Source Guard

IP Source Guard

You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor and you can enable IP source guard when DHCP snooping is enabled on an untrusted interface.

After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping.

The switch uses a source IP lookup table in hardware to bind IP addresses to ports. For IP and MAC filtering, a combination of source IP and source MAC lookups are used. IP traffic with a source IP address in the binding table is allowed, all other traffic is denied.

The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.
IP Source Guard for Static Hosts

Do not use IPSG (IP source guard) for static hosts on uplink ports or trunk ports.

IPSG for static hosts extends the IPSG capability to non-DHCP and static environments. The previous IPSG used the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. This security feature restricts IP traffic on nonrouted Layer 2 interfaces. It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings. The previous version of IPSG required a DHCP environment for IPSG to work.

IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IPSG for static hosts also supports dynamic hosts. If a dynamic host receives a DHCP-assigned IP address that is available in the IP DHCP snooping table, the same entry is learned by the IP device tracking table. When you enter the EXEC command, the IP device tracking table displays the entries as ACTIVE.

Some IP hosts with multiple network interfaces can inject some invalid packets into a network interface. The invalid packets contain the IP or MAC address for another network interface of the host as the source address. The invalid packets can cause IPSG for static hosts to connect to the host, to learn the invalid IP or MAC address bindings, and to reject the valid bindings. Consult the vendor of the corresponding operating system and the network interface to prevent the host from injecting invalid packets.

IPSG for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP address. To resolve hosts that have moved or gone away for any reason, IPSG for static hosts leverages IP device tracking to age out dynamically learned IP address bindings. This feature can be used with DHCP snooping. Multiple bindings are established on a port that is connected to both DHCP and static hosts. For example, bindings are stored in both the device tracking database as well as in the DHCP snooping binding database.

IP Source Guard Configuration Guidelines

- You can configure static IP bindings only on nonrouted ports. If you enter the `ip source binding mac-address vlan vlan-id ip-address interface interface-id` global configuration command on a routed interface, this error message appears:

  Static IP source binding can only be configured on switch port.
• When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.

• If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.

Note: If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

• You can enable this feature when 802.1x port-based authentication is enabled.

How to Configure IP Source Guard

Enabling IP Source Guard

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. ip verify source [port-security ]
5. exit
6. ip source binding mac-address vlan vlan-id ip-address interface interface-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>
<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><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><strong>Step 3</strong></td>
<td>Specifies the interface to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
PurposeCommand or Action

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

Step 4 ip verify source [port-security ]
Example:
Switch(config-if)# ip verify source

Step 5 exit
Example:
Switch(config-if)# exit

Step 6 ip source binding mac-address vlan vlan-id ip-address interface interface-id
Example:
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1

Step 7 end
Example:
Switch(config)# end

Step 8 show running-config
Example:
Switch# show running-config

Step 9 copy running-config startup-config
Example:
Switch# copy running-config startup-config

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

You must configure the ip device tracking maximum limit-number interface configuration command globally for IPSG for static hosts to work. If you only configure this command on a port without enabling IP device tracking globally or by setting an IP device tracking maximum on that interface, IPSG with static hosts rejects all the IP traffic from that interface.
### SUMMARY STEPS

1. enable
2. configure terminal
3. ip device tracking
4. interface interface-id
5. switchport mode access
6. switchport access vlan vlan-id
7. ip verify source[tracking] [port-security ]
8. ip device tracking maximum number
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.  
  Example:  
  Switch> enable |  
  • Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** ip device tracking | Turns on the IP host table, and globally enables IP device tracking.  
  Example:  
  Switch(config)# ip device tracking |
| **Step 4** interface interface-id | Enters interface configuration mode.  
  Example:  
  Switch(config)# interface gigabitethernet 1/0/1 |
| **Step 5** switchport mode access | Configures a port as access.  
  Example:  
  Switch(config-if)# switchport mode access |
| **Step 6** switchport access vlan vlan-id | Configures the VLAN for this port.  
  Example:  
  |
### Monitoring IP Source Guard

#### Step 7

**ip verify source [tracking] [port-security]**

*Example:*

```plaintext
Switch(config-if)# ip verify source tracking port-security
```

Enables IP source guard with source IP address filtering. (Optional) `tracking`—Enables IP source guard for static hosts. (Optional) `port-security`—Enables MAC address filtering. The command `ip verify source tracking port-security` enables IP source guard for static hosts with MAC address filtering.

#### Step 8

**ip device tracking maximum number**

*Example:*

```plaintext
Switch(config-if)# ip device tracking maximum 8
```

Establishes a maximum limit for the number of static IPs that the IP device tracking table allows on the port. The range is 1 to 10. The maximum number is 10.

**Note** You must configure the `ip device tracking maximum limit-number` interface configuration command.

#### Step 9

**end**

*Example:*

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

returns to privileged EXEC mode.

---

### Monitoring IP Source Guard

#### Table 91: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip verify source [interface interface-id]</code></td>
<td>Displays the IP source guard configuration on the switch or on a specific interface.</td>
</tr>
<tr>
<td>`show ip device tracking {all</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>

#### Table 92: Interface Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip verify source tracking</code></td>
<td>Verifies the data source.</td>
</tr>
</tbody>
</table>

For detailed information about the fields in these displays, see the command reference for this release.
### 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 the 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>
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 819
- Information About 802.1x Port-Based Authentication, on page 819
- How to Configure 802.1x Port-Based Authentication, on page 843
- Monitoring 802.1x Statistics and Status, on page 886
- Additional References for IEEE 802.1x Port-Based Authentication, on page 887
- Feature Information for 802.1x Port-Based Authentication, on page 888

**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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Information About 802.1x Port-Based Authentication**

The 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

---

**Note**

TACACS is not supported with 802.1x authentication.
Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

<table>
<thead>
<tr>
<th>Client session</th>
<th>Maximum sessions supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum dot1x or MAB client sessions</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum web-based authentication sessions</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum dot1x sessions with critical-auth VLAN enabled and server re-initialized</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum MAB sessions with various session features applied</td>
<td>2000</td>
</tr>
<tr>
<td>Maximum dot1x sessions with service templates or session features applied</td>
<td>2000</td>
</tr>
</tbody>
</table>

**Port-Based Authentication Process**

To configure IEEE 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.

The AAA process begins with authentication. When 802.1x port-based authentication is enabled and the client supports 802.1x-compliant client software, these events occur:

- If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network.
- If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can use the client MAC address for authorization. If the client MAC address is valid and the authorization succeeds, the switch grants the client access to the network. If the client MAC address is invalid and the authorization fails, the switch assigns the client to a guest VLAN that provides limited services if a guest VLAN is configured.
- If the switch gets an invalid identity from an 802.1x-capable client and a restricted VLAN is specified, the switch can assign the client to a restricted VLAN that provides limited services.
- If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN.

**Note**

Inaccessible authentication bypass is also referred to as critical authentication or the AAA fail policy.

If Multi Domain Authentication (MDA) is enabled on a port, this flow can be used with some exceptions that are applicable to voice authorization.
This figure shows the authentication process.

The switch re-authenticates a client when one of these situations occurs:

- Periodic re-authentication is enabled, and the re-authentication timer expires.

You can configure the re-authentication timer to use a switch-specific value or to be based on values from the RADIUS server.

After 802.1x authentication using a RADIUS server is configured, the switch uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which re-authentication occurs.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during re-authentication. The actions are Initialize and ReAuthenticate. When the Initialize action is set (the attribute value is DEFAULT), the 802.1x session ends, and connectivity is lost during re-authentication. When the ReAuthenticate action is set (the attribute value is RADIUS-Request), the session is not affected during re-authentication.

- You manually re-authenticate the client by entering the `dot1x re-authenticate interface interface-id` privileged EXEC command.
Port-Based Authentication Initiation and Message Exchange

During 802.1x authentication, the switch or the client can initiate authentication. If you enable authentication on a port by using the `authentication port-control auto` interface configuration command, the switch initiates authentication when the link state changes from down to up or periodically as long as the port remains up and unauthenticated. The switch sends an EAP-request/identity frame to the client to request its identity. Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client’s identity.

Note

If 802.1x authentication is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted.

The specific exchange of EAP frames depends on the authentication method being used.

Figure 62: Message Exchange

This figure shows a message exchange initiated by the client when the client uses the One-Time-Password (OTP) authentication method with a RADIUS server.

If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can authorize the client when the switch detects an Ethernet packet from the
client. The switch uses the MAC address of the client as its identity and includes this information in the RADIUS-access/request frame that is sent to the RADIUS server. After the server sends the switch the RADIUS-access/accept frame (authorization is successful), the port becomes authorized. If authorization fails and a guest VLAN is specified, the switch assigns the port to the guest VLAN. If the switch detects an EAPOL packet while waiting for an Ethernet packet, the switch stops the MAC authentication bypass process and starts 802.1x authentication.

*Figure 63: Message Exchange During MAC Authentication Bypass*

This figure shows the message exchange during MAC authentication bypass.

![Message Exchange During MAC Authentication Bypass](image)

**Authentication Manager for Port-Based Authentication**

**Port-Based Authentication Methods**

*Table 93: 802.1x Features*

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Mode</th>
<th>Single host</th>
<th>Multiple host</th>
<th>MDA</th>
<th>Multiple Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
</tr>
<tr>
<td></td>
<td>Per-user ACL</td>
<td></td>
<td></td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
</tr>
<tr>
<td></td>
<td>Filter-ID attribute</td>
<td></td>
<td></td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
</tr>
<tr>
<td></td>
<td>Downloadable ACL</td>
<td></td>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td></td>
<td>Redirect URL</td>
<td></td>
<td></td>
<td>Redirect URL</td>
<td>Redirect URL</td>
</tr>
</tbody>
</table>
## Per-User ACLs and Filter-Ids

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Mode</th>
<th>Single host</th>
<th>Multiple host</th>
<th>MDA</th>
<th>Multiple Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC authentication</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
</tr>
<tr>
<td>bypass</td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
</tr>
<tr>
<td></td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
</tr>
<tr>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td></td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
</tr>
<tr>
<td>Standalone web</td>
<td>Proxy ACL, Filter-ID attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-ID attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-ID attribute, downloadable ACL</td>
<td>Proxy ACL, Filter-ID attribute, downloadable ACL</td>
<td></td>
</tr>
<tr>
<td>authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
</tr>
<tr>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td></td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
</tr>
<tr>
<td>NAC Layer 2 IP</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
</tr>
<tr>
<td>validation</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
</tr>
<tr>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td></td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
</tr>
<tr>
<td>Web authentication</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
</tr>
<tr>
<td>as fallback method</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
</tr>
<tr>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td></td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
<td>Redirect URL</td>
</tr>
<tr>
<td>11</td>
<td>Supported in Cisco IOS Release 12.2(50)SE and later.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>For clients that do not support 802.1x authentication.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Per-User ACLs and Filter-Ids

**Note**

You can only set any as the source in the ACL.

**Note**

For any ACL configured for multiple-host mode, the source portion of statement must be any. (For example, `permit icmp any host 10.10.1.1`.)

You must specify any in the source ports of any defined ACL. Otherwise, the ACL cannot be applied and authorization fails. Single host is the only exception to support backward compatibility.

More than one host can be authenticated on MDA-enabled and multi-auth ports. The ACL policy applied for one host does not effect the traffic of another host. If only one host is authenticated on a multi-host port, and the other hosts gain network access without authentication, the ACL policy for the first host can be applied to the other connected hosts by specifying any in the source address.
Port-Based Authentication Manager CLI Commands

The authentication-manager interface-configuration commands control all the authentication methods, such as 802.1x, MAC authentication bypass, and web authentication. The authentication manager commands determine the priority and order of authentication methods applied to a connected host.

The authentication manager commands control generic authentication features, such as host-mode, violation mode, and the authentication timer. Generic authentication commands include the authentication host-mode, authentication violation, and authentication timer interface configuration commands.

802.1x-specific commands begin with the dot1x keyword. For example, the authentication port-control auto interface configuration command enables authentication on an interface.

To disable dot1x on a switch, remove the configuration globally by using the no dot1x system-auth-control, and also remove it from all configured interfaces.

Note

If 802.1x authentication is globally disabled, other authentication methods are still enabled on that port, such as web authentication.

The authentication manager commands provide the same functionality as earlier 802.1x commands.

When filtering out verbose system messages generated by the authentication manager, the filtered content typically relates to authentication success. You can also filter verbose messages for 802.1x authentication and MAB authentication. There is a separate command for each authentication method:

- The no authentication logging verbose global configuration command filters verbose messages from the authentication manager.
- The no dot1x logging verbose global configuration command filters 802.1x authentication verbose messages.
- The no mab logging verbose global configuration command filters MAC authentication bypass (MAB) verbose messages.

Table 94: Authentication Manager Commands and Earlier 802.1x Commands

<table>
<thead>
<tr>
<th>The authentication manager commands in Cisco IOS Release 12.2(50)SE or later</th>
<th>The equivalent 802.1x commands in Cisco IOS Release 12.2(46)SE and earlier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication control-direction {both</td>
<td>in}</td>
<td>dot1x control-direction {both</td>
</tr>
<tr>
<td>authentication event</td>
<td>dot1x auth-fail vlan</td>
<td>Enable the restricted VLAN on a port.</td>
</tr>
<tr>
<td></td>
<td>dot1x critical (interface configuration)</td>
<td>Enable the inaccessible-authentication-bypass feature.</td>
</tr>
<tr>
<td></td>
<td>dot1x guest-vlan6</td>
<td>Specify an active VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td>Authentication Manager Commands in Cisco IOS Release 12.2(50)SE or Later</td>
<td>Equivalent 802.1X Commands in Cisco IOS Release 12.2(46)SE and Earlier</td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><code>authentication fallback fallback-profile</code></td>
<td><code>dot1x fallback fallback-profile</code></td>
<td>Configure a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.</td>
</tr>
<tr>
<td>`authentication host-mode {multi-auth</td>
<td>multi-domain</td>
<td>multi-host</td>
</tr>
<tr>
<td><code>authentication order mab</code></td>
<td><code>dot1x order mab</code></td>
<td>Provides the flexibility to define the order of authentication methods to be used.</td>
</tr>
<tr>
<td><code>authentication periodic</code></td>
<td><code>dot1x reauthentication</code></td>
<td>Enable periodic re-authentication of the client.</td>
</tr>
<tr>
<td>`authentication port-control {auto</td>
<td>force-authorized</td>
<td>force-unauthorized}`</td>
</tr>
<tr>
<td><code>authentication timer</code></td>
<td><code>dot1x timeout</code></td>
<td>Set the 802.1x timers.</td>
</tr>
<tr>
<td>`authentication violation {protect</td>
<td>restrict</td>
<td>shutdown}`</td>
</tr>
</tbody>
</table>

## Ports in Authorized and Unauthorized States

During 802.1x authentication, depending on the switch port state, the switch can grant a client access to the network. The port starts in the unauthorized state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress and egress traffic except for 802.1x authentication, CDP, and STP packets. When a client is successfully authenticated, the port changes to the authorized state, allowing all traffic for the client to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and 802.1x protocol packets before the client is successfully authenticated.

### Note

CDP bypass is not supported and may cause a port to go into err-disabled state.

If a client that does not support 802.1x authentication connects to an unauthorized 802.1x port, the switch requests the client’s identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1x-enabled client connects to a port that is not running the 802.1x standard, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the
client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the `authentication port-control` interface configuration command and these keywords:

- **force-authorized**—disables 802.1x authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.

- **force-unauthorized**—causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

- **auto**—enables 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client MAC address.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to change to the unauthorized state.

If the link state of a port changes from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

### 802.1x Host Mode

You can configure an 802.1x port for single-host or for multiple-hosts mode. In single-host mode, only one client can be connected to the 802.1x-enabled switch port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

In multiple-hosts mode, you can attach multiple hosts to a single 802.1x-enabled port. In this mode, only one of the attached clients must be authorized for all clients to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), the switch denies network access to all of the attached clients.

In this topology, the wireless access point is responsible for authenticating the clients attached to it, and it also acts as a client to the switch.

*Figure 64: Multiple Host Mode Example*
For all host modes, the line protocol stays up before authorization when port-based authentication is configured. The switch supports multidomain authentication (MDA), which allows both a data device and a voice device, such as an IP Phone (Cisco or non-Cisco), to connect to the same switch port.

### 802.1x Multiple Authentication Mode

Multiple-authentication (multiauth) mode allows multiple authenticated clients on the data VLAN and voice VLAN. Each host is individually authenticated. There is no limit to the number of data or voice device that can be authenticated on a multiauth port.

If a hub or access point is connected to an 802.1x-enabled port, each connected client must be authenticated. For non-802.1x devices, you can use MAC authentication bypass or web authentication as the per-host authentication fallback method to authenticate different hosts with different methods on a single port.

When a port is in multiple-authentication mode, the authentication-failed VLAN features do not activate.

You can assign a RADIUS-server-supplied VLAN in multi-auth mode, under the following conditions:

- The host is the first host authorized on the port, and the RADIUS server supplies VLAN information
- Subsequent hosts are authorized with a VLAN that matches the operational VLAN.
- A host is authorized on the port with no VLAN assignment, and subsequent hosts either have no VLAN assignment, or their VLAN information matches the operational VLAN.
- The first host authorized on the port has a group VLAN assignment, and subsequent hosts either have no VLAN assignment, or their group VLAN matches the group VLAN on the port. Subsequent hosts must use the same VLAN from the VLAN group as the first host. If a VLAN list is used, all hosts are subject to the conditions specified in the VLAN list.
- After a VLAN is assigned to a host on the port, subsequent hosts must have matching VLAN information or be denied access to the port.
- You cannot configure a guest VLAN or an auth-fail VLAN in multi-auth mode.
- The behavior of the critical-auth VLAN is not changed for multi-auth mode. When a host tries to authenticate and the server is not reachable, all authorized hosts are reinitialized in the configured VLAN.

### MAC Move

When a MAC address is authenticated on one switch port, that address is not allowed on another authentication manager-enabled port of the switch. If the switch detects that same MAC address on another authentication manager-enabled port, the address is not allowed.

There are situations where a MAC address might need to move from one port to another on the same switch. For example, when there is another device (for example a hub or an IP phone) between an authenticated host and a switch port, you might want to disconnect the host from the device and connect it directly to another port on the same switch.
You can globally enable MAC move so the device is reauthenticated on the new port. When a host moves to a second port, the session on the first port is deleted, and the host is reauthenticated on the new port. MAC move is supported on all host modes. (The authenticated host can move to any port on the switch, no matter which host mode is enabled on the that port.) When a MAC address moves from one port to another, the switch terminates the authenticated session on the original port and initiates a new authentication sequence on the new port. The MAC move feature applies to both voice and data hosts.

**Note**
In open authentication mode, a MAC address is immediately moved from the original port to the new port, with no requirement for authorization on the new port.

## MAC Replace

The MAC replace feature can be configured to address the violation that occurs when a host attempts to connect to a port where another host was previously authenticated.

**Note**
This feature does not apply to ports in multi-auth mode, because violations are not triggered in that mode. It does not apply to ports in multiple host mode, because in that mode, only the first host requires authentication.

The MAC replace feature can be configured to address the violation that occurs when a host attempts to connect to a port where another host was previously authenticated.

If you configure the `authentication violation` interface configuration command with the `replace` keyword, the authentication process on a port in multi-domain mode is:

- A new MAC address is received on a port with an existing authenticated MAC address.
- The authentication manager replaces the MAC address of the current data host on the port with the new MAC address.
- The authentication manager initiates the authentication process for the new MAC address.
- If the authentication manager determines that the new host is a voice host, the original voice host is removed.

If a port is in open authentication mode, any new MAC address is immediately added to the MAC address table.

## 802.1x Accounting

The 802.1x standard defines how users are authorized and authenticated for network access but does not keep track of network usage. 802.1x accounting is disabled by default. You can enable 802.1x accounting to monitor this activity on 802.1x-enabled ports:

- User successfully authenticates.
- User logs off.
- Link-down occurs.
- Re-authentication successfully occurs.
- Re-authentication fails.
The switch does not log 802.1x accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

**802.1x Accounting Attribute-Value Pairs**

The information sent to the RADIUS server is represented in the form of Attribute-Value (AV) pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.)

AV pairs are automatically sent by a switch that is configured for 802.1x accounting. Three types of RADIUS accounting packets are sent by a switch:

- **START**—sent when a new user session starts
- **INTERIM**—sent during an existing session for updates
- **STOP**—sent when a session terminates

You can view the AV pairs that are being sent by the switch by entering the `debug radius accounting` privileged EXEC command. For more information about this command, see the *Cisco IOS Debug Command Reference, Release 12.4*.

This table lists the AV pairs and when they are sent:

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>AV Pair Name</th>
<th>START</th>
<th>INTERIM</th>
<th>STOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute[1]</td>
<td>User-Name</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[4]</td>
<td>NAS-IP-Address</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[5]</td>
<td>NAS-Port</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[8]</td>
<td>Framed-IP-Address</td>
<td>Never</td>
<td>Sometimes(^{13})</td>
<td>Sometimes</td>
</tr>
<tr>
<td>Attribute[25]</td>
<td>Class</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[30]</td>
<td>Called-Station-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[31]</td>
<td>Calling-Station-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[40]</td>
<td>Acct-Status-Type</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[41]</td>
<td>Acct-Delay-Time</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[42]</td>
<td>Acct-Input-Octets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[43]</td>
<td>Acct-Output-Octets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[47]</td>
<td>Acct-Input-Packets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[48]</td>
<td>Acct-Output-Packets</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[44]</td>
<td>Acct-Session-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
</tbody>
</table>
### Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their hostname or IP address, hostname and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which 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, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

### 802.1x Authentication with VLAN Assignment

The switch supports 802.1x authentication with VLAN assignment. After successful 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the client connected to the switch port. You can use this feature to limit network access for certain users.

Voice device authentication is supported with multidomain host mode in Cisco IOS Release 12.2(37)SE. In Cisco IOS Release 12.2(40)SE and later, when a voice device is authorized and the RADIUS server returned an authorized VLAN, the voice VLAN on the port is configured to send and receive packets on the assigned voice VLAN. Voice VLAN assignment behaves the same as data VLAN assignment on multidomain authentication (MDA)-enabled ports.

When configured on the switch and the RADIUS server, 802.1x authentication with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server or if 802.1x authentication is disabled, the port is configured in its access VLAN after successful authentication. Recall that an access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.

- If 802.1x authentication is enabled but the VLAN information from the RADIUS server is not valid, authorization fails and configured VLAN remains in use. This prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.

Configuration errors could include specifying a VLAN for a routed port, a malformed VLAN ID, a nonexistent or internal (routed port) VLAN ID, an RSPAN VLAN, a shut down or suspended VLAN. In the case of a multidomain host port, configuration errors can also be due to an attempted assignment of a data VLAN that matches the configured or assigned voice VLAN ID (or the reverse).

- If 802.1x authentication is enabled and all information from the RADIUS server is valid, the authorized device is placed in the specified VLAN after authentication.

#### Attribute Table

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>AV Pair Name</th>
<th>START</th>
<th>INTERIM</th>
<th>STOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute[45]</td>
<td>Acct-Authentic</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[46]</td>
<td>Acct-Session-Time</td>
<td>Never</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[49]</td>
<td>Acct-Terminate-Cause</td>
<td>Never</td>
<td>Never</td>
<td>Always</td>
</tr>
<tr>
<td>Attribute[61]</td>
<td>NAS-Port-Type</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
</tbody>
</table>

13 The Framed-IP-Address AV pair is sent when a valid static IP address is configured or when a Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.
• If the multiple-hosts mode is enabled on an 802.1x port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.

• Enabling port security does not impact the RADIUS server-assigned VLAN behavior.

• If 802.1x authentication is disabled on the port, it is returned to the configured access VLAN and configured voice VLAN.

• If an 802.1x port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect. In the case of a multidomain host, the same applies to voice devices when the port is fully authorized with these exceptions:
  • If the VLAN configuration change of one device results in matching the other device configured or assigned VLAN, then authorization of all devices on the port is terminated and multidomain host mode is disabled until a valid configuration is restored where data and voice device configured VLANs no longer match.
  • If a voice device is authorized and is using a downloaded voice VLAN, the removal of the voice VLAN configuration, or modifying the configuration value to dot1p or untagged results in voice device un-authorization and the disablement of multi-domain host mode.

When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is put into the configured access VLAN.

If an 802.1x port is authenticated and put in the RADIUS server-assigned VLAN, any change to the port access VLAN configuration does not take effect. In the case of a multidomain host, the same applies to voice devices when the port is fully authorized with these exceptions:
  • If the VLAN configuration change of one device results in matching the other device configured or assigned VLAN, authorization of all devices on the port is terminated and multidomain host mode is disabled until a valid configuration is restored where data and voice device configured VLANs no longer match.
  • If a voice device is authorized and is using a downloaded voice VLAN, the removal of the voice VLAN configuration, or modifying the configuration value to dot1p or untagged results in voice device un-authorization and the disablement of multi-domain host mode.

When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is put into the configured access 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 VLAN Membership Policy Server (VMPS).

To configure VLAN assignment you need to perform these tasks:
  • Enable AAA authorization by using the network keyword to allow interface configuration from the RADIUS server.
  • Enable 802.1x authentication. (The VLAN assignment feature is automatically enabled when you configure 802.1x authentication on an access port).
  • Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch:
    • [64] Tunnel-Type = VLAN
    • [65] Tunnel-Medium-Type = 802
    • [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID
802.1x Authentication with Guest VLAN

You can configure a guest VLAN for each 802.1x port on the switch to provide limited services to clients, such as downloading the 802.1x client. These clients might be upgrading their system for 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x-capable.

When you enable a guest VLAN on an 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

The switch maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an IEEE 802.1x-capable supplicant, and the interface does not change to the guest VLAN state. EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, the interface changes to the guest VLAN state.

If the switch is trying to authorize an 802.1x-capable voice device and the AAA server is unavailable, the authorization attempt fails, but the detection of the EAPOL packet is saved in the EAPOL history. When the AAA server becomes available, the switch authorizes the voice device. However, the switch no longer allows other devices access to the guest VLAN. To prevent this situation, use one of these command sequences:

- Enter the `authentication event no-response action authorize vlan vlan-id` interface configuration command to allow access to the guest VLAN.
- Enter the `shutdown` interface configuration command followed by the `no shutdown` interface configuration command to restart the port.

If devices send EAPOL packets to the switch during the lifetime of the link, the switch no longer allows clients that fail authentication access to the guest VLAN.

---

Note

If an EAPOL packet is detected after the interface has changed to the guest VLAN, the interface reverts to an unauthorized state, and 802.1x authentication restarts.

Any number of 802.1x-incapable clients are allowed access when the switch port is moved to the guest VLAN. If an 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on 802.1x ports in single host, multiple host, multi-auth and multi-domain modes.

The switch supports MAC authentication bypass. When MAC authentication bypass is enabled on an 802.1x port, the switch can authorize clients based on the client MAC address when IEEE 802.1x authentication times out while waiting for an EAPOL message exchange. After detecting a client on an 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is specified.
802.1x Authentication with Restricted VLAN

You can configure a restricted VLAN (also referred to as an authentication failed VLAN) for each IEEE 802.1x port on a switch to provide limited services to clients that cannot access the guest VLAN. These clients are 802.1x-compliant and cannot access another VLAN because they fail the authentication process. A restricted VLAN allows users without valid credentials in an authentication server (typically, visitors to an enterprise) to access a limited set of services. The administrator can control the services available to the restricted VLAN.

**Note**

You can configure a VLAN to be both the guest VLAN and the restricted VLAN if you want to provide the same services to both types of users.

Without this feature, the client attempts and fails authentication indefinitely, and the switch port remains in the spanning-tree blocking state. With this feature, you can configure the switch port to be in the restricted VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator counts the failed authentication attempts for the client. When this count exceeds the configured maximum number of authentication attempts, the port moves to the restricted VLAN. The failed attempt count increments when the RADIUS server replies with either an EAP failure or an empty response without an EAP packet. When the port moves into the restricted VLAN, the failed attempt counter resets.

Users who fail authentication remain in the restricted VLAN until the next re-authentication attempt. A port in the restricted VLAN tries to re-authenticate at configured intervals (the default is 60 seconds). If re-authentication fails, the port remains in the restricted VLAN. If re-authentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable re-authentication. If you do this, the only way to restart the authentication process is for the port to receive a link down or EAP logoff event. We recommend that you keep re-authentication enabled if a client might connect through a hub. When a client disconnects from the hub, the port might not receive the link down or EAP logoff event.

After a port moves to the restricted VLAN, a simulated EAP success message is sent to the client. This prevents clients from indefinitely attempting authentication. Some clients (for example, devices running Windows XP) cannot implement DHCP without EAP success.

Restricted VLANs are supported on 802.1x ports in all host modes and on Layer 2 ports.

Other security port features such as dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.

802.1X Auth Fail VLAN

You can configure an auth fail VLAN for each 802.1X port on a switch to provide limited services to clients that cannot access the guest VLAN. These clients are 802.1X-compliant and cannot access another VLAN because they fail the authentication process. An auth fail VLAN allows users without valid credentials in an authentication server (typically, visitors to an enterprise) to access a limited set of services. The administrator can control the services available to the auth fail VLAN.

**Note**

You can configure a VLAN to be both the guest VLAN and the auth fail VLAN if you want to provide the same services to both types of users.
Without this feature, the client attempts and fails authentication indefinitely, and the switch port remains in the spanning-tree blocking state. With this feature, you can configure the switch port to be in the auth fail VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator counts the failed authentication attempts for the client. When this count exceeds the configured maximum number of authentication attempts, the port moves to the auth fail VLAN. The failed attempt count increments when the RADIUS server replies with either an EAP failure or an empty response without an EAP packet. When the port moves into the auth fail VLAN, the failed attempt counter resets.

Users who fail authentication remain in the auth fail VLAN until the next reauthentication attempt. A port in the auth fail VLAN tries to reauthenticate at configured intervals (the default is 60 seconds). If reauthentication fails, the port remains in the auth fail VLAN. If reauthentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable reauthentication. If you do this, the only way to restart the authentication process is for the port to receive a link down or EAP logoff event. It is recommended that you keep reauthentication enabled if a client might connect through a hub. When a client disconnects from the hub, the port might not receive the link down or EAP logoff event.

After a port moves to the auth fail VLAN, a simulated EAP success message is sent to the client. This prevents clients from indefinitely attempting authentication.

As a prerequisite, the switch must be connected to a Cisco secure Access Control System (ACS) and RADIUS authentication, authorization, and accounting (AAA) must be configured for Web authentication. If appropriate, you must enable ACL download.

802.1x Authentication with Inaccessible Authentication Bypass

Use the inaccessible authentication bypass feature, also referred to as critical authentication or the AAA fail policy, when the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated. You can configure the switch to connect those hosts to critical ports.

When a new host tries to connect to the critical port, that host is moved to a user-specified access VLAN, the critical VLAN. The administrator gives limited authentication to the hosts.

When the switch tries to authenticate a host connected to a critical port, the switch checks the status of the configured RADIUS server. If a server is available, the switch can authenticate the host. However, if all the RADIUS servers are unavailable, the switch grants network access to the host and puts the port in the critical-authentication state, which is a special case of the authentication state.

Note

If critical authentication is configured on interface, then vlan used for critical authorization (critical vlan) should be active on the switch. If the critical vlan is inactive (or) down, critical authentication session will keep trying to enable inactive vlan and fail repeatedly. This can lead to large amount of memory holding.

Inaccessible Authentication Bypass Support on Multiple-Authentication Ports

When a port is configured on any host mode and the AAA server is unavailable, the port is then configured to multi-host mode and moved to the critical VLAN. To support this inaccessible bypass on multiple-authentication (multiauth) ports, use the authentication event server dead action reinitialize vlan vlan-id command. When a new host tries to connect to the critical port, that port is reinitialized and all the connected hosts are moved to the user-specified access VLAN.

This command is supported on all host modes.
Inaccessible Authentication Bypass Authentication Results

The behavior of the inaccessible authentication bypass feature depends on the authorization state of the port:

- If the port is unauthorized when a host connected to a critical port tries to authenticate and all servers are unavailable, the switch puts the port in the critical-authentication state on the RADIUS-configured or user-specified access VLAN.

- If the port is already authorized and reauthentication occurs, the switch puts the critical port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.

- If the RADIUS server becomes unavailable during an authentication exchange, the current exchange times out, and the switch puts the critical port in the critical-authentication state during the next authentication attempt.

You can configure the critical port to reinitialize hosts and move them out of the critical VLAN when the RADIUS server is again available. When this is configured, all critical ports in the critical-authentication state are automatically re-authenticated.

Inaccessible Authentication Bypass Feature Interactions

Inaccessible authentication bypass interacts with these features:

- Guest VLAN—Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on 8021.x port, the features interact as follows:
  - If at least one RADIUS server is available, the switch assigns a client to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.
  - If all the RADIUS servers are not available and the client is connected to a critical port, the switch authenticates the client and puts the critical port in the critical-authentication state on the RADIUS-configured or user-specified access VLAN.
  - If all the RADIUS servers are not available and the client is not connected to a critical port, the switch might not assign clients to the guest VLAN if one is configured.
  - If all the RADIUS servers are not available and if a client is connected to a critical port and was previously assigned to a guest VLAN, the switch keeps the port in the guest VLAN.

- Restricted VLAN—If the port is already authorized in a restricted VLAN and the RADIUS servers are unavailable, the switch puts the critical port in the critical-authentication state in the restricted VLAN.

- 802.1x accounting—Accounting is not affected if the RADIUS servers are unavailable.

- Voice VLAN—Inaccessible authentication bypass is compatible with voice VLAN, but the RADIUS-configured or user-specified access VLAN and the voice VLAN must be different.

- Remote Switched Port Analyzer (RSPAN)—Do not configure an RSPAN VLAN as the RADIUS-configured or user-specified access VLAN for inaccessible authentication bypass.
802.1x Critical Voice VLAN

When an IP phone connected to a port is authenticated by the Cisco Identity Services Engine (ISE), the phone is put into the voice domain. If the ISE is not reachable, the switch cannot determine if the device is a voice device. If the server is unavailable, the phone cannot access the voice network and therefore cannot operate.

For data traffic, you can configure inaccessible authentication bypass, or critical authentication, to allow traffic to pass through on the native VLAN when the server is not available. If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network and puts the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. When the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated, the switch connects those hosts to critical ports. A new host trying to connect to the critical port is moved to a user-specified access VLAN, the critical VLAN, and granted limited authentication.

You can enter the `authentication event server dead action authorize voice` interface configuration command to configure the critical voice VLAN feature. When the ISE does not respond, the port goes into critical authentication mode. When traffic coming from the host is tagged with the voice VLAN, the connected device (the phone) is put in the configured voice VLAN for the port. The IP phones learn the voice VLAN identification through Cisco Discovery Protocol (Cisco devices) or through LLDP or DHCP.

You can configure the voice VLAN for a port by entering the `switchport voice vlan vlan-id` interface configuration command.

This feature is supported in multidomain and multi-auth host modes. Although you can enter the command when the switch in single-host or multi-host mode, the command has no effect unless the device changes to multidomain or multi-auth host mode.

802.1x User Distribution

You can configure 802.1x user distribution to load-balance users with the same group name across multiple different VLANs.

The VLANs are either supplied by the RADIUS server or configured through the switch CLI under a VLAN group name.

- Configure the RADIUS server to send more than one VLAN name for a user. The multiple VLAN names can be sent as part of the response to the user. The 802.1x user distribution tracks all the users in a particular VLAN and achieves load balancing by moving the authorized user to the least populated VLAN.

- Configure the RADIUS server to send a VLAN group name for a user. The VLAN group name can be sent as part of the response to the user. You can search for the selected VLAN group name among the VLAN group names that you configured by using the switch CLI. If the VLAN group name is found, the corresponding VLANs under this VLAN group name are searched to find the least populated VLAN. Load balancing is achieved by moving the corresponding authorized user to that VLAN.

Note: The RADIUS server can send the VLAN information in any combination of VLAN-IDs, VLAN names, or VLAN groups.
802.1x User Distribution Configuration Guidelines

- Confirm that at least one VLAN is mapped to the VLAN group.
- You can map more than one VLAN to a VLAN group.
- You can modify the VLAN group by adding or deleting a VLAN.
- When you clear an existing VLAN from the VLAN group name, none of the authenticated ports in the VLAN are cleared, but the mappings are removed from the existing VLAN group.
- If you clear the last VLAN from the VLAN group name, the VLAN group is cleared.
- You can clear a VLAN group even when the active VLANs are mapped to the group. When you clear a VLAN group, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.

IEEE 802.1x Authentication with Voice VLAN Ports

A voice VLAN port is a special access port associated with two VLAN identifiers:

- VVID to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- PVID to carry the data traffic to and from the workstation connected to the switch through the IP phone. The PVID is the native VLAN of the port.

The IP phone uses the VVID for its voice traffic, regardless of the authorization state of the port. This allows the phone to work independently of IEEE 802.1x authentication.

In single-host mode, only the IP phone is allowed on the voice VLAN. In multiple-hosts mode, additional clients can send traffic on the voice VLAN after a supplicant is authenticated on the PVID. When multiple-hosts mode is enabled, the supplicant authentication affects both the PVID and the VVID.

A voice VLAN port becomes active when there is a link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several IP phones are connected in series, the switch recognizes only the one directly connected to it. When IEEE 802.1x authentication is enabled on a voice VLAN port, the switch drops packets from unrecognized IP phones more than one hop away.

When IEEE 802.1x authentication is enabled on a switch port, you can configure an access port VLAN that is also a voice VLAN.

When IP phones are connected to an 802.1x-enabled switch port that is in single host mode, the switch grants the phones network access without authenticating them. We recommend that you use multidomain authentication (MDA) on the port to authenticate both a data device and a voice device, such as an IP phone.

---

**Note**

If you enable IEEE 802.1x authentication on an access port on which a voice VLAN is configured and to which a Cisco IP Phone is connected, the Cisco IP phone loses connectivity to the switch for up to 30 seconds.
IEEE 802.1x Authentication with Port Security

In general, Cisco does not recommend enabling port security when IEEE 802.1x is enabled. Since IEEE 802.1x enforces a single MAC address per port (or per VLAN when MDA is configured for IP telephony), port security is redundant and in some cases may interfere with expected IEEE 802.1x operations.

IEEE 802.1x Authentication with MAC Authentication Bypass

You can configure the switch to authorize clients based on the client MAC address by using the MAC authentication bypass feature. For example, you can enable this feature on IEEE 802.1x ports connected to devices such as printers.

If IEEE 802.1x authentication times out while waiting for an EAPOL response from the client, the switch tries to authorize the client by using MAC authentication bypass.

When the MAC authentication bypass feature is enabled on an IEEE 802.1x port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. After detecting a client on an IEEE 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is configured. This process works for most client devices; however, it does not work for clients that use an alternate MAC address format.

You can configure how MAB authentication is performed for clients with MAC addresses that deviate from the standard format or where the RADIUS configuration requires the user name and password to differ.

If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an 802.1x-capable supplicant and uses 802.1x authentication (not MAC authentication bypass) to authorize the interface. EAPOL history is cleared if the interface link status goes down.

If the switch already authorized a port by using MAC authentication bypass and detects an IEEE 802.1x supplicant, the switch does not unauthorize the client connected to the port. When re-authentication occurs, the switch uses the authentication or re-authentication methods configured on the port, if the previous session ended because the Termination-Action RADIUS attribute value is DEFAULT.

Clients that were authorized with MAC authentication bypass can be re-authenticated. The re-authentication process is the same as that for clients that were authenticated with IEEE 802.1x. During re-authentication, the port remains in the previously assigned VLAN. If re-authentication is successful, the switch keeps the port in the same VLAN. If re-authentication fails, the switch assigns the port to the guest VLAN, if one is configured.

If re-authentication is based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]) and if the Termination-Action RADIUS attribute (Attribute [29]) action is Initialize (the attribute value is DEFAULT), the MAC authentication bypass session ends, and connectivity is lost during re-authentication. If MAC authentication bypass is enabled and the IEEE 802.1x authentication times out, the switch uses the MAC authentication bypass feature to initiate re-authorization. For more information about these AV pairs, see RFC 3580, “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.”

MAC authentication bypass interacts with the features:

• IEEE 802.1x authentication—You can enable MAC authentication bypass only if 802.1x authentication is enabled on the port.

• Guest VLAN—If a client has an invalid MAC address identity, the switch assigns the client to a guest VLAN if one is configured.
• Restricted VLAN—This feature is not supported when the client connected to an IEEE 802.1x port is authenticated with MAC authentication bypass.

• Port security

• Voice VLAN

Per-User ACLs Authentication through 802.1x/MAB/WebAuth Users

You can enable per-user access control lists (ACLs) to provide different levels of network access and service to an 802.1x-authenticated user. When the RADIUS server authenticates a user connected to an 802.1x port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1x port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are inacl#<n> for the ingress direction and outacl#<n> for the egress direction. MAC ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It does not support port ACLs in the egress direction on Layer 2 ports.

Use only the extended ACL syntax style to define the per-user configuration stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if you use the Filter-Id attribute, it can point to a standard ACL.

You can use the Filter-Id attribute to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by .in for ingress filtering or .out for egress filtering. If the RADIUS server does not allow the .in or .out syntax, the access list is applied to the outbound ACL by default. The user is marked unauthorized if the filter-Id sent from the RADIUS server is not configured on the device. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered in the range of 1 to 199 (IP standard ACLs) and 1300 to 2699 (IP extended ACLs).

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

You must meet the following prerequisites to configure per-user ACLs:

• Enable AAA authentication.

• Enable AAA authorization by using the network keyword to allow interface configuration from the RADIUS server.

• Enable 802.1x authentication.

• Configure the user profile and VSAs on the RADIUS server.

Flexible Authentication Ordering

You can use flexible authentication ordering to configure the order of methods that a port uses to authenticate a new host. The IEEE 802.1X Flexible Authentication feature supports three authentication methods:

• dot1X—IEEE 802.1X authentication is a Layer 2 authentication method.
• **mab**—MAC-Authentication Bypass is a Layer 2 authentication method.

• **webauth**—Web authentication is a Layer 3 authentication method.

Using this feature, you can control which ports use which authentication methods, and you can control the failover sequencing of methods on those ports. For example, MAC authentication bypass and 802.1x can be the primary or secondary authentication methods, and web authentication can be the fallback method if either or both of those authentication attempts fail.

The IEEE 802.1X Flexible Authentication feature supports the following host modes:

• **multi-auth**—Multiauthentication allows one authentication on a voice VLAN and multiple authentications on the data VLAN.

• **multi-domain**—Multidomain authentication allows two authentications: one on the voice VLAN and one on the data VLAN.

---

**Open1x Authentication**

Open1x authentication allows a device access to a port before that device is authenticated. When open authentication is configured, a new host can pass traffic according to the access control list (ACL) defined on the port. After the host is authenticated, the policies configured on the RADIUS server are applied to that host.

You can configure open authentication with these scenarios:

• **Single-host mode with open authentication**—Only one user is allowed network access before and after authentication.

• **MDA mode with open authentication**—Only one user in the voice domain and one user in the data domain are allowed.

• **Multiple-hosts mode with open authentication**—Any host can access the network.

• **Multiple-authentication mode with open authentication**—Similar to MDA, except multiple hosts can be authenticated.

---

**Note**

If open authentication is configured, it takes precedence over other authentication controls. This means that if you use the `authentication open` interface configuration command, the port will grant access to the host irrespective of the `authentication port-control` interface configuration command.

---

**Multidomain Authentication**

The switch supports multidomain authentication (MDA), which allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port. The port is divided into a data domain and a voice domain.
For all host modes, the line protocol stays up before authorization when port-based authentication is configured.

MDA does not enforce the order of device authentication. However, for best results, we recommend that a voice device is authenticated before a data device on an MDA-enabled port.

Follow these guidelines for configuring MDA:

- You must configure a switch port for MDA.
- You must configure the voice VLAN for the IP phone when the host mode is set to multidomain.
- Voice VLAN assignment on an MDA-enabled port is supported Cisco IOS Release 12.2(40)SE and later.
- To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of device-traffic-class=voice. Without this value, the switch treats the voice device as a data device.
- The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
- If more than one device attempts authorization on either the voice or the data domain of a port, it is error disabled.
- Until a device is authorized, the port drops its traffic. Non-Cisco IP phones or voice devices are allowed into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending on the voice VLAN, its access to the data VLAN is blocked.
- A voice device MAC address that is binding on the data VLAN is not counted towards the port security MAC address limit.
- MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect to devices that do not support IEEE 802.1x authentication.
- When a data or a voice device is detected on a port, its MAC address is blocked until authorization succeeds. If the authorization fails, the MAC address remains blocked for 5 minutes.
- If more than five devices are detected on the data VLAN or more than one voice device is detected on the voice VLAN while a port is unauthorized, the port is error disabled.
- When a port host mode is changed from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone that has been allowed on the port voice VLAN is automatically removed and must be reauthenticated on that port.
- Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port changes from single- or multihost mode to multidomain mode.
- Switching a port host mode from multidomain to single- or multihost mode removes all authorized devices from the port.
- If a data domain is authorized first and placed in the guest VLAN, non-IEEE 802.1x-capable voice devices need to tag their packets on the voice VLAN to trigger authentication.
- We do not recommend per-user ACLs with an MDA-enabled port. An authorized device with a per-user ACL policy might impact traffic on both the voice and data VLANs of the port. If used, only one device on the port should enforce per-user ACLs.
Limiting Login for Users

The Limiting Login feature helps Network administrators to limit the login attempt of users to a network. When a user fails to successfully login to a network within a configurable number of attempts within a configurable time limit, the user can be blocked. This feature is enabled only for local users and not for remote users. You need to configure the `aaa authentication rejected` command in global configuration mode to enable this feature.

Voice Aware 802.1x Security

To use voice aware IEEE 802.1x authentication, the switch must be running the LAN base image.

You use the voice aware 802.1x security feature to configure the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. In previous releases, when an attempt to authenticate the data client caused a security violation, the entire port shut down, resulting in a complete loss of connectivity.

You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

How to Configure 802.1x Port-Based Authentication

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>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>Feature</td>
<td>Default Setting</td>
</tr>
<tr>
<td>---------------------------------------------</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>
<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>
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) destination ports—You can enable 802.1x authentication on a port that is a SPAN destination port. However, 802.1x authentication is disabled until the port is removed as a SPAN destination port. You can enable 802.1x authentication on a SPAN 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.

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, or dynamic ports.

- You can configure any VLAN except 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.
  • 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.
  • You can configure any VLAN except 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.

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 Voice Aware 802.1x Security

To use voice aware IEEE 802.1x authentication, the switch must be running the LAN base image.

You use the voice aware 802.1x security feature on the switch to disable only the VLAN on which a security violation occurs, whether it is a data or voice VLAN. You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN results in the shutdown of only the data VLAN. The traffic on the voice VLAN flows through the switch without interruption.

Follow these guidelines to configure voice aware 802.1x voice security on the switch:

- You enable voice aware 802.1x security by entering the `errdisable detect cause security-violation shutdown vlan` global configuration command. You disable voice aware 802.1x security by entering the `no` version of this command. This command applies to all 802.1x-configured ports in the switch.

  Note: If you do not include the `shutdown vlan` keywords, the entire port is shut down when it enters the error-disabled state.

- If you use the `errdisable recovery cause security-violation` global configuration command to configure error-disabled recovery, the port is automatically re-enabled. If error-disabled recovery is not configured for the port, you re-enable it by using the `shutdown` and `no shutdown` interface configuration commands.

- You can re-enable individual VLANs by using the `clear errdisable interface interface-id vlan [vlan-list]` privileged EXEC command. If you do not specify a range, all VLANs on the port are enabled.

Beginning in privileged EXEC mode, follow these steps to enable voice aware 802.1x security:

**SUMMARY STEPS**

1. configure terminal
2. errdisable detect cause security-violation shutdown vlan
3. errdisable recovery cause security-violation
4. clear errdisable interface interface-id vlan [vlan-list]
5. Enter the following:
   a. shutdown
   b. no shutdown
6. end
7. show errdisable detect

**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> errdisable detect cause security-violation shutdown vlan</td>
<td>Shut down any VLAN on which a security violation error occurs.</td>
</tr>
</tbody>
</table>
## 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:

### Example

This example shows how to configure the switch to shut down any VLAN on which a security violation error occurs:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

This example shows how to re-enable all VLANs that were error disabled on port Gigabit Ethernet 40/2.

```
Switch# clear errdisable interface gigabitethernet40/2
```

You can verify your settings by entering the `show errdisable detect` privileged EXEC command.

### Configuring 802.1x Violation Modes

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> errdisable recovery cause security-violation</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 4** clear errdisable interface interface-id vlan [vlan-list] | (Optional) Reenable individual VLANs that have been error disabled.  
  - For interface-id specify the port on which to reenable individual VLANs.  
  - (Optional) For vlan-list specify a list of VLANs to be re-enabled. If vlan-list is not specified, all VLANs are re-enabled. |
| **Step 5** Enter the following:               | (Optional) Re-enable an error-disabled VLAN, and clear all error-disable indications.  
  - shutdown  
  - no shutdown |
| **Step 6** end                                | Return to privileged EXEC mode. |
| **Step 7** show errdisable detect             | Verify your entries. |

**Note** If the `shutdown vlan` keywords are not included, the entire port enters the error-disabled state and shuts down.
**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}  
7. 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 aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 3 aaa authentication dot1x {default} method1</td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa authentication dot1x default group radius</td>
<td>To create a default list that is used when a named list is not specified in the <strong>authentication</strong> command, use the <strong>default</strong> keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports. For <strong>method1</strong>, enter the <strong>group radius</strong> keywords to use the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td>Step 4 interface interface-id</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>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 0/4</td>
<td></td>
</tr>
<tr>
<td>Step 5 switchport mode access</td>
<td>Sets the port to access mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td>Step 6 authentication violation {shutdown</td>
<td>restrict</td>
</tr>
</tbody>
</table>
| Example: | *

*shutdown*—Error disable the port.
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>Step 1</td>
<td>A user connects to a port on the switch.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Authentication is performed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Returns to privileged EXEC mode.
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>The switch sends a start message to an accounting server.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Re-authentication is performed, as necessary.</td>
</tr>
<tr>
<td>Step 6</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>Step 7</td>
<td>The user disconnects from the port.</td>
</tr>
<tr>
<td>Step 8</td>
<td>The switch sends a stop message to the accounting server.</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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</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>Step 2</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Creates an 802.1x authentication method list.</td>
</tr>
<tr>
<td>aaa authentication dot1x {default} method1</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

To create a default list that is used when a named list is not specified in the `authentication` command, use the `default` keyword followed by the method that is to be used in default situations. The default method list is automatically applied to all ports.

For `method1`, enter the `group radius` keywords to use the list of all RADIUS servers for authentication.

- **Note** Though other keywords are visible in the command-line help string, only the `group radius` keywords are supported.

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# aaa authentication dot1x default group radius</code></td>
<td>Enables 802.1x authentication globally on the switch.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>dot1x system-auth-control</code></td>
<td>Enables 802.1x authentication globally on the switch.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# dot1x system-auth-control</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <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>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# aaa authorization network default group radius</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>radius-server host ip-address</code></td>
<td>(Optional) Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# radius-server host 124.2.2.12</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <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>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# radius-server key abc1234</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> <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>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# interface gigabitethernet 0/2</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> <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>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config-if)# switchport mode access</code></td>
<td></td>
</tr>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
Step 10 | Enables 802.1x authentication on the port.
authentication port-control auto | Enables 802.1x authentication on the port.

**Example:**
```
Switch(config-if)# authentication port-control auto
```

Step 11 | Sets the interface Port Access Entity to act only as an authenticator and ignore messages meant for a supplicant.
dot1x pae authenticator | Sets the interface Port Access Entity to act only as an authenticator and ignore messages meant for a supplicant.

**Example:**
```
Switch(config-if)# dot1x pae authenticator
```

Step 12 | Returns to privileged EXEC mode.
end | Returns to privileged EXEC mode.

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

---

### 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>
</table>
| Step 1 | Enables privileged EXEC mode.
`enable` | Enables privileged EXEC mode. |
### 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></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></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>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `radius-server host {hostname | ip-address} auth-port port-number key string` | Configures the RADIUS server parameters.
| **Example:**      |         |
| Switch(config)# `radius-server host 125.5.5.43 auth-port 1645 key rad123` | 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`             | Returns to privileged EXEC mode. |
| **Example:**      |         |
| Switch(config)# `end` |         |
### SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. authentication host-mode [multi-auth | multi-domain | multi-host | single-host]
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>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 port to which multiple hosts are indirectly attached, and enter interface configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td></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></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:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication host-mode multi-host</td>
<td></td>
</tr>
<tr>
<td><em>multi-auth</em>—Allow multiple authenticated clients on both the voice VLAN and data VLAN.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The <em>multi-auth</em> keyword is only available with the <em>authentication host-mode</em> command.</td>
</tr>
<tr>
<td><em>multi-host</em>—Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You must configure the voice VLAN for the IP phone when the host mode is set to <em>multi-domain</em>.</td>
</tr>
<tr>
<td><em>multi-domain</em>—Allow both a host and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an IEEE 802.1x-authorized port.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Make sure that the <em>authentication port-control</em> interface configuration command is set to <em>auto</em> for the specified interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
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><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:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

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

| **Step 3**                        |                                                                        |
| `authentication periodic`         | Enables periodic re-authentication of the client, which is disabled by default. |
| Example:                          |                                                                        |
| `Switch(config-if)# authentication periodic` |                                                                        |

| **Step 4**                        |                                                                        |
| `authentication timer {{[inactivity | reauthenticate | restart | unauthorized]} {value}}` | Sets the number of seconds between re-authentication attempts. |
| Example:                          |                                                                        |

**Note** The default value is 3600 seconds. To change the value of the reauthentication timer or to have the switch use a RADIUS-provided session timeout, enter the `authentication timer reauthenticate` command.


## Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Switch(config-if)# authentication timer reauthenticate 180 | • **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  
|                                    | • **restart value**—Interval in seconds after which an attempt is made to authenticate an unauthorized port  
|                                    | • **unauthorized value**—Interval in seconds after which an unauthorized session will get deleted  

This command affects the behavior of the switch only if periodic re-authentication is enabled.

### Step 5

**Example:**

Switch(config-if)# end

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

---

## 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>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></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>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** | interface interface-id  
Example: | Specifies the port to be configured, and enter interface configuration mode. |
| | Switch(config)# interface gigabitethernet 0/1 |
| **Step 3** | authentication timer restart seconds  
Example: | Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. |
| | Switch(config-if)# authentication timer restart 30 |
| **Step 4** | end  
Example: | Returns to privileged EXEC mode. |
| | Switch(config-if)# end |
| **Step 5** | show authentication sessions interface interface-id  
Example: | Verifies your entries. |
| | Switch# show authentication sessions interface gigabitethernet 0/1 |
| **Step 6** | copy running-config startup-config  
Example: | (Optional) Saves your entries in the configuration file. |
| | Switch# copy running-config startup-config |

### 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 resend 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
Changing the Switch-to-Client Retransmission Time

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></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>Switch# <code>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><code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# <code>interface gigabitethernet 0/1</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></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><code>authentication timer reauthenticate seconds</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-if)# <code>authentication timer reauthenticate 60</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><strong>Example:</strong></td>
<td>Switch(config-if)# <code>end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>show authentication sessions interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>show authentication sessions interface gigabitethernet 0/1</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# <code>copy running-config startup-config</code></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.

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 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>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>
<tr>
<td><strong>Step 3</strong> dot1x max-reauth-req count</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>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# dot1x max-reauth-req 5</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-if)# end</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 0/1</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>
</tbody>
</table>
Enabling MAC Move

MAC move allows an authenticated host to move from one port on the switch to another.

Beginning in privileged EXEC mode, follow these steps to globally enable MAC move on the switch. This procedure is optional.

**SUMMARY STEPS**

1. configure terminal
2. authentication mac-move permit
3. end
4. show running-config
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:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>authentication mac-move permit</th>
<th>Enables MAC move on the switch. Default is deny.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
<td>In Session Aware Networking mode, the default CLI is access-session mac-move deny. To enable Mac Move in Session Aware Networking, use the no access-session mac-move global configuration command. In legacy mode (IBNS 1.0), default value for mac-move is deny and in C3PL mode (IBNS 2.0) default value is permit.</td>
</tr>
<tr>
<td>Switch(config)# authentication mac-move permit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>show running-config</th>
<th>Verifies your entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enabling MAC Replace

MAC replace allows a host to replace an authenticated host on a port.

Beginning in privileged EXEC mode, follow these steps to enable MAC replace on an interface. This procedure is optional.

**SUMMARY STEPS**

1. configure terminal
2. interface interface-id
3. authentication violation {protect | replace | restrict | shutdown}
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>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 0/2</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>authentication violation {protect</td>
<td>replace</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication violation replace</td>
<td></td>
</tr>
</tbody>
</table>

The other keywords have these effects:

- **protect**: the port drops packets with unexpected MAC addresses without generating a system message.
- **restrict**: violating packets are dropped by the CPU and a system message is generated.
### 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.**

**Note**

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. 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</td>
</tr>
<tr>
<td>Example:</td>
<td>mode.</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>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:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# aaa accounting dot1x default start-stop group</td>
<td></td>
</tr>
<tr>
<td>radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>aaa accounting system default start-stop group radius</td>
<td>(Optional) Enables system accounting (using the list of all RADIUS</td>
</tr>
<tr>
<td>Example:</td>
<td>servers) and generates system accounting reload event messages when</td>
</tr>
<tr>
<td>Switch(config-if)# aaa accounting system default start-stop group</td>
<td>the switch reloads.</td>
</tr>
<tr>
<td>radius</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>
<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>
</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`
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>Switch# configure terminal</td>
</tr>
</tbody>
</table>

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

| **Step 3** | 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. |
| `authentication event no-response action authorize vlan vlan-id` | |
| Example: | Switch(config-if)# authentication event no-response action authorize vlan 2 |

| **Step 4** | Returns to privileged EXEC mode. |
| `end` | |
| Example: | |
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>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</td>
</tr>
<tr>
<td>Example:</td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 0/2</td>
<td></td>
</tr>
<tr>
<td>Step 3 authentication port-control auto</td>
<td>Enables 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td>Step 4 authentication event fail action authorize vlan</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>vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication event fail action</td>
<td></td>
</tr>
<tr>
<td>authorize vlan 2</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`
6. `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 0/3</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>Example:</td>
<td></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Example:</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-server dead-time minutes`
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>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

---

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.

#### Step 5

**authentication event retry retry count**

Example:

```
Switch(config-if)# authentication event retry 2
```

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.

#### Step 6

**end**

Example:

```
Switch(config-if)# end
```

Returns to privileged EXEC mode.
<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 2**

aaa new-model

**Example:**

Switch(config)# aaa new-model

**Sets the conditions that determine when a RADIUS server is considered unavailable or down (dead).**

- **time**—1 to 120 seconds. The switch dynamically determines a default *seconds* value between 10 and 60.

- **number**—1 to 100 tries. The switch dynamically determines a default *tries number* between 10 and 100.

**Step 3**

radius-server dead-criteria {time seconds} [tries number]

**Example:**

Switch(config)# radius-server dead-criteria time 20 tries 10

(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.

**Step 4**

radius-server dead-time minutes

**Example:**

Switch(config)# radius-server dead-time 60

(Optional) Configure the RADIUS server parameters by using these keywords:

- **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.

**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**—Enable automated testing of the RADIUS server status, and specify the username to be used.

- **idle-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).
### Command or Action | Purpose
--- | ---
| • ignore-acct-port — Disable testing on the RADIUS-server accounting port. |  
| • ignore-auth-port — Disable testing on the RADIUS-server authentication port. |  
| • For **keystring**, 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 {eap0 | recovery delay milliseconds}**  
**Example:**  
`Switch(config)# dot1x critical eapol`  
`(config)# dot1x critical recovery delay 2000`

(Optional) Configure the parameters for inaccessible authentication bypass:

- **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:**  

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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Switch(config-if)# authentication event server`
| `dead action`
| `reinitialize vlan 20` | *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:**

```
Switch(config-if)# do copy running-config
startup-config
```

(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 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>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 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>authentication port-control auto</td>
<td>Enables 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# authentication port-control auto</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>mab [eap]</td>
<td>Enables MAC authentication bypass.</td>
</tr>
<tr>
<td>(Optional) Use the eap keyword to configure the switch to use EAP for authorization.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# mab</td>
<td></td>
</tr>
</tbody>
</table>
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 attribute 1 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>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 format of the MAC address in the User-Name attribute of MAB-generated Access-Request packets.</td>
</tr>
<tr>
<td>`mab request format attribute 1 groupsize {1</td>
<td>2</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# mab request format attribute 1 groupsize 12</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Per-User ACLs Authentication through 802.1x/MAB/WebAuth Users

To configure a switch to accept downloadable ACLs or redirect URLs from the RADIUS server during authentication of an attached host, perform this task.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip device tracking
4. aaa new-model
5. aaa authorization network default group radius
6. radius-server vsa send authentication
7. interface interface-id
8. ip access-group acl-id in
9. end
10. show running-config interface interface-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>Step 3</td>
<td></td>
</tr>
<tr>
<td>mab request format attribute2 {0</td>
<td>7} text</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# mab request format attribute 2 7 A02f44E18B12</td>
<td></td>
</tr>
<tr>
<td>Step 4</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>
</tbody>
</table>

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
<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> ip device tracking</td>
<td>Enables the IP device tracking table.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ip device tracking</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> aaa authorization network default group radius</td>
<td>Sets the authorization method. To remove the authorization method, use the <strong>no aaa authorization network default group radius</strong> command.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authorization network default group radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> radius-server vsa send authentication</td>
<td>Configures the network access server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# radius-server vsa send authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> interface interface-id</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> ip access-group acl-id in</td>
<td>Configures the default ACL on the port in the input direction. Applicable only for WebAuth Users; dynamically available for 8.2.1x and MAB authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ip access-group 99 in</td>
<td>Note: The ACL ID is an access list name or number.</td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Returns to Privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong> show running-config interface interface-id</td>
<td>Displays the specific interface configuration for verification.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config interface interface-id</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> copy running-config startup-config</td>
<td>(Optional) Save entries in the configuration file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
Example: Per-User ACLs Authentication through 802.1x/MAB/WebAuth Users

The following example shows how to configure a switch for a downloadable policy:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface fastEthernet 2/13
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

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>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>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 authentication, authorization, and accounting (AAA) access control model.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# aaa new-model</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><strong>aaa authentication login default local</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;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><strong>aaa authentication rejected n in m ban x</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;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.&lt;br&gt;• <code>n</code>—Specifies the number of times a user can try to login.&lt;br&gt;• <code>m</code>—Specifies the number of seconds within which an user can try to login.&lt;br&gt;• <code>x</code>—Specifies the time period an user is banned if the user fails to successfully login.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device(config)# end</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>show aaa local user blocked</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# show aaa local user blocked</td>
<td>Displays the list of local users who were blocked.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>clear aaa local user blocked username username</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# clear aaa local user blocked username user1</td>
<td>Clears the information about the blocked local user.</td>
</tr>
</tbody>
</table>

**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 802.1X Auth Fail VLAN**

Perform this optional task to configure an auth fail VLAN.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface type slot/port`
3. `access-session port-control auto`
4. `authentication event fail action authorize vlan vlan-id`
5. `end`
6. `show access-session interface interface-id`
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# configure terminal | Enters global configuration mode. |
| **Step 2**
**Example:**
Switch(config)# interface gigabitethernet0/1 | Specifies the port to be configured, and enters interface configuration mode. |
| **Step 3**
**Example:**
Switch(config-if)# access-session port-control auto | Enables 802.1X authentication on the port. |
| **Step 4**
**Example:**
Switch(config-if)# authentication event fail action authorize vlan 40 | Specifies an active VLAN as an 802.1X auth fail VLAN. The range is 1 to 4094. |
| **Step 5**
**Example:**
Switch(config-if)# end | Returns to privileged EXEC mode. |
| **Step 6**
**Example:**
Switch# show access-session interface gigabitethernet0/1 | (Optional) Verify your entries. |
| **Step 7**
**Example:**
Switch# copy running-config startup-config | (Optional) Saves your entries in the configuration file. |
What to do next

To disable and remove the auth fail VLAN, use the `no authentication event fail` interface configuration command. The port returns to the default state.

### Configuring the Number of Authentication Retries

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.

Perform this optional task to configure the maximum number of allowed authentication attempts.

### SUMMARY STEPS

1. `configure terminal`
2. `interface interface-id`
3. `access-session port-control auto`
4. `authentication event fail action authorize vlan vlan-id`
5. `authentication event fail retry retry-count`
6. `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:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><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 enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet0/1</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>access-session port-control auto</code></td>
<td>Enables 802.1X authentication on the port.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# access-session port-control auto</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>authentication event fail action authorize vlan vlan-id</code></td>
<td>Specifies an active VLAN as an 802.1X auth fail VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config-if)# authentication event fail action authorize vlan 40</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td><strong>authentication event fail retry</strong> <em>retry-count</em></td>
<td>Specifies a number of authentication attempts before a port moves to the auth fail VLAN. The range is 0 to 5, and the default is 2 attempts after the initial failed event.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication event fail retry 4</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><strong>end</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to set 2 as the number of authentication attempts allowed before the port moves to the auth fail VLAN:

Switch(config-if)# authentication event retry 2

---

**Configuring Flexible Authentication Ordering**

The examples used in the instructions below change the order of Flexible Authentication Ordering so that MAB is attempted before IEEE 802.1X authentication (dot1x). MAB is configured as the first authentication method, so MAB will have priority over all other authentication methods.

---

**Note**


Beginning in privileged EXEC mode, follow these steps:

**SUMMARY STEPS**

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport mode access**
4. **authentication order** [ **dot1x** | **mab** ] | {**webauth**}
5. **authentication priority** [ **dot1x** | **mab** ] | {**webauth**}
6. **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><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: Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> authentication order [ dot1x</td>
<td>mab ]</td>
</tr>
<tr>
<td>Example: Switch(config-if)# authentication order mab dot1x</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> authentication priority [ dot1x</td>
<td>mab ]</td>
</tr>
<tr>
<td>Example: Switch(config-if)# authentication priority mab dot1x</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>
</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
### Detailed Steps

<table>
<thead>
<tr>
<th></th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>configure terminal</strong></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><strong>interface interface-id</strong></td>
<td>Specifies the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>switchport mode access</strong></td>
<td>Sets the port to access mode only if you configured the RADIUS server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>**authentication control-direction {both</td>
<td>in}**</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-if)# authentication control-direction both</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><strong>authentication fallback name</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>Example:</td>
<td>Switch(config-if)# authentication fallback profile</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>**authentication host-mode [multi-auth</td>
<td>multi-domain</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>Switch(config-if)# authentication host-mode multi-auth</td>
<td>(Optional) Enables or disable open access on a port.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> authentication open</td>
<td>(Optional) Sets the order of authentication methods used on a port.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# authentication open</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> authentication order [ dot1x</td>
<td>mab ]</td>
<td>(Optional) Enables or disable reauthentication on a port.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# authentication order dot1x webauth</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> authentication periodic</td>
<td>(Optional) Enables manual control of the port authorization state.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# authentication periodic</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> authentication port-control {auto</td>
<td>force-authorized</td>
<td>force-un-authorized}</td>
</tr>
<tr>
<td>Example: Switch(config-if)# authentication port-control auto</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>Example: Switch(config-if)# end</td>
<td></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
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></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>Enters interface configuration mode, and specify the port to be configured.</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 3</strong></td>
<td></td>
</tr>
<tr>
<td>dot1x default</td>
<td>Resets the 802.1x parameters to the default values.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# dot1x default</td>
<td></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-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring 802.1x Statistics and Status

**Table 97: Privileged EXEC show Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot1x all statistics</td>
<td>Displays 802.1x statistics for all ports</td>
</tr>
<tr>
<td>show dot1x interface interface-id statistics</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>show dot1x interface interface-id</td>
<td>Displays the 802.1x administrative and operational status for a specific port</td>
</tr>
</tbody>
</table>

**Table 98: Global Configuration Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>no dot1x logging verbose</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 for IEEE 802.1x Port-Based Authentication**

<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 the 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 for 802.1x Port-Based Authentication

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supports the use of same authorization methods on all the</td>
</tr>
<tr>
<td></td>
<td>Catalyst switches in a network.</td>
</tr>
<tr>
<td></td>
<td>Supports filtering verbose system messages from the</td>
</tr>
<tr>
<td></td>
<td>authentication manager.</td>
</tr>
</tbody>
</table>
Configuring IPv6 First Hop Security

- Finding Feature Information, on page 889
- Prerequisites for First Hop Security in IPv6, on page 889
- Restrictions for First Hop Security in IPv6, on page 890
- Information about First Hop Security in IPv6, on page 890
- How to Configure an IPv6 Snooping Policy, on page 891
- How to Configure the IPv6 Binding Table Content, on page 895
- How to Configure an IPv6 Neighbor Discovery Inspection Policy, on page 897
- How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on a Device, on page 901
- How to Configure an IPv6 Router Advertisement Guard Policy, on page 903
- How to Configure an IPv6 DHCP Guard Policy, on page 908
- How to Configure IPv6 Source Guard, on page 912
- How to Configure IPv6 Prefix Guard, on page 915
- Configuration Examples for IPv6 First Hop Security, on page 918
- Additional References, on page 919

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 First Hop Security in IPv6

- You have configured the necessary IPv6 enabled SDM template.

- QoS should be enabled on the switch before configuring CoPP policies using mls qos command.
Restrictions for First Hop Security in IPv6

- The following restrictions apply when applying FHS policies to EtherChannel interfaces (Port Channels):
  - A physical port with an FHS policy attached cannot join an EtherChannel group.
  - An FHS policy cannot be attached to an physical port when it is a member of an EtherChannel group.

- By default, a snooping policy has a security-level of guard. When such a snooping policy is configured on an access switch, external IPv6 Router Advertisement (RA) or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server packets are blocked, even though the uplink port facing the router or DHCP server/relay is configured as a trusted port. To allow IPv6 RA or DHCPv6 server messages, do the following:
  - Apply an IPv6 RA-guard policy (for RA) or IPv6 DHCP-guard policy (for DHCP server messages) on the uplink port.
  - Configure a snooping policy with a lower security-level, for example glean or inspect. However, configuring a lower security level is not recommended with such a snooping policy, because benefits of First Hop security features are not effective.

- The following restrictions apply for CoPP policies with IPv6 SISF-based device tracking policies due to limitation reported in CSCvk32439:
  - CoPP policies are required to limit IPv6 NDP traffic when IPv6 SISF policies are configured on the switch.
  - After NDP CoPP policies are configured, limited traffic hits CPU. To accommodate the total end points connected, the number of NDP CoPP policies should be slightly more than the number of users connected to each switch in a stack. If you configure NDP CoPP policies less than the number of end points connected to the switch, the IP allocation to the end point is delayed but is not ignored completely.

  [Note]
  For example, if a stack of 5 switches has approximately 300 users, the NDP CoPP policies should be more than 300.

- The DHCPv6 (server-to-client and client-to-server) CoPP policies are required only if Lightweight DHCPv6 Relay Agent (LDRA) is configured under IPv6 SISF-based device tracking policies on the switch.

Information about First Hop Security in IPv6

First Hop Security in IPv6 (FHS IPv6) is a set of IPv6 security features, the policies of which can be attached to a physical interface, an EtherChannel interface, or a VLAN. An IPv6 software policy database service stores and accesses these policies. When a policy is configured or modified, the attributes of the policy are stored or updated in the software policy database, then applied as was specified. The following IPv6 policies are currently supported:
IPv6 Snooping Policy—IPv6 Snooping Policy acts as a container policy that enables most of the features available with FHS in IPv6.

IPv6 FHS Binding Table Content—A database table of IPv6 neighbors connected to the switch is created from information sources such as Neighbor Discovery (ND) protocol snooping. This database, or binding, table is used by various IPv6 guard features (such as IPv6 ND Inspection) to validate the link-layer address (LLA), the IPv4 or IPv6 address, and prefix binding of the neighbors to prevent spoofing and redirect attacks.

IPv6 Neighbor Discovery Inspection—IPv6 ND inspection learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes neighbor discovery messages in order to build a trusted binding table database and IPv6 neighbor discovery messages that do not conform are dropped. An ND message is considered trustworthy if its IPv6-to-Media Access Control (MAC) mapping is verifiable.

This feature mitigates some of the inherent vulnerabilities of the ND mechanism, such as attacks on DAD, address resolution, router discovery, and the neighbor cache.

IPv6 Router Advertisement Guard—The IPv6 Router Advertisement (RA) guard feature enables the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network switch platform. RAs are used by routers to announce themselves on the link. The RA Guard feature analyzes the RAs and filters out bogus RAs sent by unauthorized routers. In host mode, all router advertisement and router redirect messages are disallowed on the port. The RA guard feature compares configuration information on the Layer 2 device with the information found in the received RA frame. Once the Layer 2 device has validated the content of the RA frame and router redirect frame against the configuration, it forwards the RA to its unicast or multicast destination. If the RA frame content is not validated, the RA is dropped.

IPv6 DHCP Guard—The IPv6 DHCP Guard feature blocks reply and advertisement messages that come from unauthorized DHCPv6 servers and relay agents. IPv6 DHCP guard can prevent forged messages from being entered in the binding table and block DHCPv6 server messages when they are received on ports that are not explicitly configured as facing a DHCPv6 server or DHCP relay. To use this feature, configure a policy and attach it to an interface or a VLAN. To debug DHCP guard packets, use the `debug ipv6 snooping dhcp-guard` privileged EXEC command.

### How to Configure an IPv6 Snooping Policy

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Snooping Policy:

**SUMMARY STEPS**

1. `configure terminal`
2. `ipv6 snooping policy policy-name`
3. `{[default ] | [device-role {node | switch }] | [limit address-count value] | [no] | [protocol {dhcp | ndp}] | [security-level {glean | guard | inspect}] | [tracking {disable [stale-lifetime {seconds | infinite}] | enable [reachable-lifetime {seconds | infinite}] } ] | [trusted-port ] }
4. `end`
5. `show ipv6 snooping policy policy-name`
## 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 the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ipv6 snooping policy <em>policy-name</em></td>
<td>Creates a snooping policy and enters IPv6 Snooping Policy Configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config)# ipv6 snooping policy example_policy</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>security-level {glean</td>
<td>guard</td>
</tr>
<tr>
<td></td>
<td>tracking {disable</td>
<td>enable}</td>
</tr>
<tr>
<td></td>
<td>trusted-port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-ipv6-snooping)# trusted-port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: Switch(config-ipv6-snooping)# security-level inspect</td>
<td></td>
</tr>
</tbody>
</table>

How to Configure an IPv6 Snooping Policy

---

Security

---

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.</td>
</tr>
</tbody>
</table>

### Step 4

**Example:**

```bash
Switch(config-ipv6-snooping)# exit
```

### Step 5

**Example:**

```bash
Switch# show ipv6 snooping policy example_policy
```

### What to do next

Attach an IPv6 Snooping policy to interfaces or VLANs.

### How to Attach an IPv6 Snooping Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Snooping policy on an interface or VLAN:

#### SUMMARY STEPS

1. `configure terminal`
2. `interface Interface_type stack/module/port`
3. `switchport`
4. `ipv6 snooping {attach-policy policy_name [ vlan {vlan_id | add vlan_ids | except vlan_ids | none | remove vlan_ids } | vlan {vlan_id | add vlan_ids | except vlan_ids | none | remove vlan_ids | all } ]}`
5. `do show running-config`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><code>interface Interface_type stack/module/port</code></td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td><code>Switch(config)# interface gigabitethernet 1/1/4</code></td>
<td></td>
</tr>
<tr>
<td><code>switchport</code></td>
<td>Enters the Switchport mode.</td>
</tr>
</tbody>
</table>
### Command or Action

```
Switch(config-if)# switchport
```

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the <code>switchport</code> interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration. The command prompt displays as <code>(config-if)#</code> in Switchport configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4

**ipv6 snooping [attach-policy policy_name [ vlan {vlan_id | add vlan_ids | except vlan_ids | none | remove vlan_ids} | vlan {vlan_id | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ]**

**Example:**
```
Switch(config-if)# ipv6 snooping
```
```
or
```
Switch(config-if)# ipv6 snooping attach-policy example_policy
```
```
or
```
Switch(config-if)# ipv6 snooping vlan 111,112
```
```
or
```
Switch(config-if)# ipv6 snooping attach-policy example_policy vlan 111,112
```

Attaches a custom IPv6 snooping policy to the interface or the specified VLANs on the interface. To attach the default policy to the interface, use the `ipv6 snooping` command without the `attach-policy` keyword. To attach the default policy to VLANs on the interface, use the `ipv6 snooping vlan` command. The default policy is, security-level `guard`, device-role `node`, protocol `ndp` and `dhcp`.

### Step 5

**do show running-config**

**Example:**
```
Switch#(config-if)# do show running-config
```

Verifies that the policy is attached to the specified interface without exiting the interface configuration mode.

---

**How to Attach an IPv6 Snooping Policy to a Layer 2 EtherChannel Interface**

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Snooping policy on an EtherChannel interface or VLAN:
## Procedure

<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 the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface range Interface_name</td>
<td>Specifies the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface range Po11</td>
<td></td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Enter the <code>do show interfaces summary</code> command for quick reference to interface names and types.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 snooping [attach-policy policy_name [vlan vlan_ids</td>
<td>Attaches the IPv6 Snooping policy to the interface or the specified VLANs on that interface. The default policy is attached if the <code>attach-policy</code> option is not used.</td>
</tr>
<tr>
<td>add vlan_ids</td>
<td>except vlan_ids</td>
</tr>
<tr>
<td>Example: Switch(config-if-range)# ipv6 snooping attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td>or Switch(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td>or Switch(config-if-range)#ipv6 snooping vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> do show running-config interface/portchannel_interface_name</td>
<td>Confirms that the policy is attached to the specified interface without exiting the configuration mode.</td>
</tr>
<tr>
<td>Example: Switch#(config-if-range)# do show running-config int po11</td>
<td></td>
</tr>
</tbody>
</table>

## How to Configure the IPv6 Binding Table Content

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content:

### SUMMARY STEPS

1. configure terminal
2. [no] ipv6 neighbor binding [vlan vlan-id {ipv6-address interface interface_type stack/module[port hw_address [reachable-lifetimevalue [seconds | default | infinite] | [tracking { [default | disable] [}]]}]

---

**Security**

**How to Configure the IPv6 Binding Table Content**

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content:

### SUMMARY STEPS

1. configure terminal
2. [no] ipv6 neighbor binding [vlan vlan-id {ipv6-address interface interface_type stack/module/port hw_address [reachable-lifetimevalue [seconds | default | infinite] | [tracking { [default | disable] [}]]}]]
### How to Configure the IPv6 Binding Table Content

**reachable-lifetimevalue** [seconds | default | infinite] | [enable reachable-lifetimevalue [seconds | default | infinite]] | [retry-interval [seconds | default | reachable-lifetimevalue [seconds | default | infinite]]]  

3. **[no]** ipv6 neighbor binding max-entries number [mac-limit number | port-limit number [mac-limit number] | vlan-limit number [mac-limit number] | [port-limit number [mac-limit-number]]]  

4. ipv6 neighbor binding logging  
5. exit  
6. show ipv6 neighbor binding

#### 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 the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> [no] ipv6 neighbor binding [vlan vlan-id</td>
<td>ipv6-address interface interface_type stack/module/port hw_address</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 neighbor binding</td>
<td>Adds a static entry to the binding table database.</td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] ipv6 neighbor binding max-entries number [mac-limit number</td>
<td>port-limit number [mac-limit number]</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 neighbor binding max-entries 30000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 neighbor binding logging</td>
<td>Enables the logging of binding table main events.</td>
</tr>
<tr>
<td>Example: Switch(config)# ipv6 neighbor binding logging</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits global configuration mode, and places the router in privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show ipv6 neighbor binding</td>
<td>Displays contents of a binding table.</td>
</tr>
<tr>
<td>Example: Switch# show ipv6 neighbor binding</td>
<td></td>
</tr>
</tbody>
</table>
How to Configure an IPv6 Neighbor Discovery Inspection Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 ND Inspection Policy:

SUMMARY STEPS

1. configure terminal
2. [no]ipv6 nd inspection policy policy-name
3. device-role {host | monitor | router | switch}
4. drop-unsecure
5. limit address-count value
6. sec-level minimum value
7. tracking [enable reachable-lifetime value | infinite] | disable stale-lifetime value infinite
8. trusted-port
9. validate source-mac
10. no {device-role | drop-unsecure | limit address-count | sec-level minimum | tracking | trusted-port | validate source-mac}
11. default {device-role | drop-unsecure | limit address-count | sec-level minimum | tracking | trusted-port | validate source-mac}
12. do show ipv6 nd inspection policy policy_name

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enters the 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>Step 2</td>
<td>Specifies the ND inspection policy name and enters ND Inspection Policy configuration mode.</td>
</tr>
<tr>
<td>[no]ipv6 nd inspection policy policy-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# ipv6 nd inspection policy example_policy</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Specifies the role of the device attached to the port. The default is host.</td>
</tr>
<tr>
<td>device-role {host</td>
<td>monitor</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-nd-inspection)# device-role switch</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Drops messages with no or invalid options or an invalid signature.</td>
</tr>
<tr>
<td>drop-unsecure</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-nd-inspection)# drop-unsecure</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Enter 1–10,000.</td>
</tr>
<tr>
<td>limit address-count value</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-nd-inspection)# limit address-count 1000</td>
<td></td>
</tr>
</tbody>
</table>
### How to Attach an IPv6 Neighbor Discovery Inspection Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 ND Inspection policy to an interface or VLANs on an interface:

#### SUMMARY STEPS

1. `configure terminal`

### Purpose Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>sec-level minimum <em>value</em></td>
<td>Specifies the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-nd-inspection)# limit address-count 1000</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>tracking {enable [reachable-lifetime {value</td>
<td>infinite}]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>disable [stale-lifetime {value</td>
<td>infinite}]</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-nd-inspection)# tracking disable stale-lifetime infinite</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>trusted-port</td>
<td>Configures a port to become a trusted port.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-nd-inspection)# trusted-port</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>validate source-mac</td>
<td>Checks the source media access control (MAC) address against the link-layer address.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-nd-inspection)# validate source-mac</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>no {device-role</td>
<td>drop-unsecure</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-nd-inspection)# no validate source-mac</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>default {device-role</td>
<td>drop-unsecure</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-nd-inspection)# default limit address-count</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>do show ipv6 nd inspection policy <em>policy_name</em></td>
<td>Verifies the ND Inspection Configuration without exiting ND inspection configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-nd-inspection)# do show ipv6 nd inspection policy example_policy</code></td>
<td></td>
</tr>
</tbody>
</table>
2. `interface Interface_type stack/module/port`

3. `ipv6 nd inspection [attach-policy policy_name [ vlan {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all } ] | vlan { {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all } ] ]`

4. `do show running-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>configure terminal</td>
<td>Enters the 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 2</td>
<td>interface Interface_type stack/module/port</td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 1/1/4</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 nd inspection [attach-policy policy_name [ vlan {vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# ipv6 nd inspection attach-policy example_policy</td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>or Switch(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224</td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>or Switch(config-if)# ipv6 nd inspection vlan 222, 223,224</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>do show running-config</td>
<td>Verifies that the policy is attached to the specified interface without exiting the interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch#(config-if)# do show running-config</td>
<td></td>
</tr>
</tbody>
</table>

### How to Attach an IPv6 Neighbor Discovery Inspection Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Neighbor Discovery Inspection policy on an EtherChannel interface or VLAN:
SUMMARY STEPS

1. configure terminal
2. interface range Interface_name
3. ipv6 nd inspection [attach-policy policy_name [ vlan {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ] | vlan [ {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ]] | vlan
   {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all}]
4. do show running-config interface portchannel_interface_name

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 the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface range Interface_name</td>
<td>Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface Po11</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** ipv6 nd inspection [attach-policy policy_name [ vlan {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ] | vlan [ {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ]] | vlan
   {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all}]
| Example: Switch(config-if-range)# ipv6 nd inspection attach-policy example_policy
or
Switch(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224
or
Switch(config-if-range)#ipv6 nd inspection vlan 222, 223,224 | Attaches the ND Inspection policy to the interface or the specified VLANs on that interface. The default policy is attached if the attach-policy option is not used. |
| **Step 4** do show running-config interface portchannel_interface_name | Confirms that the policy is attached to the specified interface without exiting the configuration mode. |
| Example: Switch#(config-if-range)# do show running-config int po11 | |
How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on a Device

To attach an IPv6 Neighbor Discovery Multicast Suppress policy on a device, complete the following steps:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ipv6 nd suppress policy *policy-name*
4. mode dad-proxy
5. mode full-proxy
6. mode mc-proxy

**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 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Step 3 ipv6 nd suppress policy <em>policy-name</em></td>
<td>Defines the Neighbor Discovery suppress policy name and enters Neighbor Discovery suppress policy configuration mode.</td>
</tr>
<tr>
<td>Step 4 mode dad-proxy</td>
<td>Enables Neighbor Discovery suppress in IPv6 DAD proxy mode.</td>
</tr>
<tr>
<td>Step 5 mode full-proxy</td>
<td>Enables Neighbor Discovery suppress to proxy multicast and unicast Neighbor Solicitation messages.</td>
</tr>
<tr>
<td>Step 6 mode mc-proxy</td>
<td>Enables Neighbor Discovery suppress to proxy multicast Neighbor Solicitation messages.</td>
</tr>
</tbody>
</table>

**How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on an Interface**

To attach an IPv6 Neighbor Discovery Multicast Suppress policy on an interface, complete the following steps:

**SUMMARY STEPS**

1. enable
2. `configure terminal`
3. Perform one of the following tasks:
   • `interface type number`
   • `ipv6 nd inspection [attach-policy policy_name [ vlan { add | except | none | remove | all } vlan [ vlan1, vlan2, vlan3... ]]]`
     OR
   • `vlan configuration vlan-id`
   • `ipv6 nd inspection [attach-policy policy_name [ vlan { add | except | none | remove | all } vlan [ vlan1, vlan2, vlan3... ]]]`

4. `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>enable</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**        | Enters the global configuration mode. |
| configure terminal | |

| **Step 3**        | Specifies an interface type and number, and places the device in interface configuration mode. |
|                   | Attaches the IPv6 Neighbor Discovery Multicast Policy to an interface or a VLAN. |
|                   | |
| Perform one of the following tasks: | |
| • `interface type number` | |
| • `ipv6 nd inspection [attach-policy policy_name [ vlan { add | except | none | remove | all } vlan [ vlan1, vlan2, vlan3... ]]]` | |
| OR | |
| • `vlan configuration vlan-id` | |
| • `ipv6 nd inspection [attach-policy policy_name [ vlan { add | except | none | remove | all } vlan [ vlan1, vlan2, vlan3... ]]]` | |

| **Step 4**        | Exists the interface configuration mode. |
| exit              | |

**How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy to a Layer 2 EtherChannel Interface**

To attach an IPv6 Neighbor Discovery Multicast Suppress policy on an EtherChannel interface, complete the following steps:
## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. Perform one of the following tasks:
   - `interface port-channel port-channel-number`
   - `ipv6 nd inspection [attach-policy policy_name [ vlan { add | except | none | remove | all } vlan [ vlan1, vlan2, vlan3...]]]`
   
   OR

   - `vlan configuration vlan-id`
   - `ipv6 nd inspection [attach-policy policy_name [ vlan { add | except | none | remove | all } vlan [ vlan1, vlan2, vlan3...]]]`

4. `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><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 the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Perform one of the following tasks:</td>
<td>Specifies an interface type and port number and places the switch in the port channel configuration mode.</td>
</tr>
<tr>
<td>- <code>interface port-channel port-channel-number</code></td>
<td>Attaches the IPv6 Neighbor Discovery Multicast Policy to an interface or a VLAN.</td>
</tr>
<tr>
<td>- `ipv6 nd inspection [attach-policy policy_name [ vlan { add</td>
<td>except</td>
</tr>
<tr>
<td>OR</td>
<td></td>
</tr>
<tr>
<td>- <code>vlan configuration vlan-id</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>- `ipv6 nd inspection [attach-policy policy_name [ vlan { add</td>
<td>except</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exists the interface configuration mode.</td>
</tr>
</tbody>
</table>

---

### How to Configure an IPv6 Router Advertisement Guard Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 Router Advertisement policy:
## Summary Steps

1. `configure terminal`
2. `[no]ipv6 nd raguard policy policy-name`
3. `[no]device-role {host | monitor | router | switch}`
4. `[no]hop-limit {maximum | minimum} value`
5. `[no]managed-config-flag {off | on}`
6. `[no]match {ipv6 access-list list | ra prefix-list list}`
7. `[no]other-config-flag {on | off}`
8. `[no]router-preference maximum {high | medium | low}`
9. `[no]trusted-port`
10. `default {device-role | hop-limit {maximum | minimum} | managed-config-flag | match {ipv6 access-list | ra prefix-list} | other-config-flag | router-preference maximum | trusted-port}`
11. `do show ipv6 nd raguard policy policy_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>Enter the global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specifies the RA Guard policy name and enters RA Guard Policy configuration mode.</td>
</tr>
<tr>
<td><code>[no]ipv6 nd raguard policy policy-name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# ipv6 nd raguard policy example_policy</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the role of the device attached to the port. The default is <code>host</code>.</td>
</tr>
<tr>
<td>`[no]device-role {host</td>
<td>monitor</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-nd-raguard)# device-role switch</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables filtering of Router Advertisement messages by the Hop Limit value. A rogue RA message may have a low Hop Limit value (equivalent to the IPv4 Time to Live) that when accepted by the host, prevents the host from generating traffic to destinations beyond the rogue RA message generator. An RA message with an unspecified Hop Limit value is blocked.</td>
</tr>
<tr>
<td>`[no]hop-limit {maximum</td>
<td>minimum} value`</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config-nd-raguard)# hop-limit maximum 33</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>If not configured, this filter is disabled. Configure <code>minimum</code> to block RA messages with Hop Limit values lower than the value you specify. Configure <code>maximum</code> to block RA messages with Hop Limit values greater than the value you specify.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enables filtering of Router Advertisement messages by the Managed Address Configuration, or &quot;M&quot; flag field. A rouge RA message with an M field of 1 can cause a host to use a rogue DHCPv6 server. If not configured, this filter is disabled.</td>
</tr>
<tr>
<td>[no]managed-config-flag {off</td>
<td>on}</td>
</tr>
<tr>
<td>Example:</td>
<td>Off—Accepts and forwards RA messages with an M value of 0, blocks those with 1.</td>
</tr>
<tr>
<td>Switch(config-nd-raguard)# managed-config-flag on</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Matches a specified prefix list or access list.</td>
</tr>
<tr>
<td>[no]match {ipv6 access-list list</td>
<td>ra prefix-list list}</td>
</tr>
<tr>
<td>Example:</td>
<td>On—Accepts and forwards RA messages with an O value of 1, blocks those with 0.</td>
</tr>
<tr>
<td>Switch(config-nd-raguard)# match ipv6 access-list example_list</td>
<td>Off—Accepts and forwards RA messages with an O value of 0, blocks those with 1.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Enables filtering of Router Advertisement messages by the Router Preference flag. If not configured, this filter is disabled.</td>
</tr>
<tr>
<td>[no]router-preference maximum {high</td>
<td>medium</td>
</tr>
<tr>
<td>Example:</td>
<td>• medium—Blocks RA messages with the Router Preference set to high.</td>
</tr>
<tr>
<td>Switch(config-nd-raguard)# router-preference maximum high</td>
<td>• low—Blocks RA messages with the Router Preference set to medium and high.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>When configured as a trusted port, all attached devices are trusted, and no further message verification is performed.</td>
</tr>
<tr>
<td>[no]trusted-port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-nd-raguard)# trusted-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Restores a command to its default value.</td>
</tr>
<tr>
<td>default {device-role</td>
<td>hop-limit {maximum</td>
</tr>
</tbody>
</table>
How to Attach an IPv6 Router Advertisement Guard Policy to an Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Router Advertisement policy to an interface or to VLANs on the interface:

### SUMMARY STEPS

1. configure terminal
2. interface Interface_type stack/module/port
3. ipv6 nd raguard [attach-policy policy_name [ vlan {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ] | vlan [ {vlan_ids | add vlan_ids | exceptvlan_ids | none | remove vlan_ids | all} ]]
4. do show running-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>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface Interface_type stack/module/port</td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>interface gigabitethernet 1/1/4</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 nd raguard [attach-policy policy_name [ vlan {vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td>ipv6 nd raguard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td>ipv6 nd raguard attach-policy example_policy vlan 222,223,224</td>
<td></td>
</tr>
</tbody>
</table>
How to Attach an IPv6 Router Advertisement Guard Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 Router Advertisement Guard Policy on an EtherChannel interface or VLAN:

SUMMARY STEPS

1. configure terminal
2. interface range  Interface_name
3. ipv6 nd raguard [attach-policy policy_name [ vlan {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ] | vlan [ {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ]]
4. do show running-config interface portchannel_interface_name

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>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 interface range  Interface_name</td>
<td>Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface Po11</td>
<td></td>
</tr>
<tr>
<td>Tip Enter the do show interfaces summary command for quick reference to interface names and types.</td>
<td></td>
</tr>
<tr>
<td>Step 3 ipv6 nd raguard [attach-policy policy_name [ vlan {vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example: Switch(config-if-range)# ipv6 nd raguard attach-policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if-range)#ipv6 nd raguard vlan 222,223,224</td>
<td></td>
</tr>
</tbody>
</table>

#### Step 4

**do show running-config**

**interface portchannel_interface_name**

**Example:**

Switch(config-if-range)# do show running-config int poll

**Confirmsthatthepolicyisattachedtothespecifiedinterface**

**withoutexitingtheconfigurationmode.**

### How to Configure an IPv6 DHCP Guard Policy

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 DHCP (DHCPv6) Guard policy:

#### SUMMARY STEPS

1. `configure terminal`
2. `[no]ipv6 dhcp guard policy policy-name`
3. `[no]device-role {client | server}`
4. `[no]match server access-list ipv6-access-list-name`
5. `[no]match reply prefix-list ipv6-prefix-list-name`
6. `[no]preference { max limit | min limit }`
7. `[no]trusted-port`
8. `default {device-role | trusted-port}`
9. `do show ipv6 dhcp guard policy policy_name`

#### 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 the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>[no]ipv6 dhcp guard policy policy-name</code></td>
<td>Specifies the DHCPv6 Guard policy name and enters DHCPv6 Guard Policy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ipv6 dhcp guard policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>
### Security

**How to Configure an IPv6 DHCP Guard Policy**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3** [no] device-role \{client | server\} | (Optional) Filters out DHCPv6 replies and DHCPv6 advertisements on the port that are not from a device of the specified role. Default is `client`.

- **client**—Default value, specifies that the attached device is a client. Server messages are dropped on this port.
- **server**—Specifies that the attached device is a DHCPv6 server. Server messages are allowed on this port.

**Example:**

Switch(config-dhcp-guard)# device-role server

| **Step 4** [no] match server access-list ipv6-access-list-name | (Optional). Enables verification that the advertised DHCPv6 server or relay address is from an authorized server access list (The destination address in the access list is 'any'). If not configured, this check will be bypassed. An empty access list is treated as a permit all.

**Example:**

`Switch(config)# ipv6 access-list my_acls
Switch(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any

Switch(config-dhcp-guard)# match server access-list my_acls`

| **Step 5** [no] match reply prefix-list ipv6-prefix-list-name | (Optional) Enables verification of the advertised prefixes in DHCPv6 reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. An empty prefix list is treated as a permit.

**Example:**

`Switch(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128

Switch(config-dhcp-guard)# match reply prefix-list my_prefix`

| **Step 6** [no] preference \{ max limit | min limit \} | Configure `max` and `min` when `device-role` is `server` to filter DHCPv6 server advertisements by the server preference value. The defaults permit all advertisements.

**Example:**

`Switch(config-dhcp-guard)# preference max 250
Switch(config-dhcp-guard)# preference min 150`

**max limit**—(0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. Default is 255. If not specified, this check will be bypassed.

**min limit**—(0 to 255) (Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. Default is 0. If not specified, this check will be bypassed.
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>[no] trusted-port</td>
<td>(Optional) trusted-port—Sets the port to a trusted mode. No further policing takes place on the port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-dhcp-guard)# trusted-port</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>default {device-role</td>
<td>trusted-port}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-dhcp-guard)# default device-role</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>do show ipv6 dhcp guard policy policy_name</td>
<td>(Optional) Displays the configuration of the IPv6 DHCP guard policy without leaving the configuration submode. Omitting the policy_name variable displays all DHCPv6 policies.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>

### Example of DHCPv6 Guard Configuration

```
enable
configure terminal
ipv6 access-list acl1
    permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
device-role server
match server access-list acl1
match reply prefix-list abc
preference min 0
preference max 255
trusted-port
interface GigabitEthernet 0/2/0
    switchport
ipv6 dhcp guard attach-policy pol1 vlan add 1
    vlan 1
ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

### How to Attach an IPv6 DHCP Guard Policy to an Interface or a VLAN on an Interface

Beginning in privileged EXEC mode, follow these steps to configure IPv6 Binding Table Content:

#### SUMMARY STEPS

1. configure terminal
2. interface Interface_type stack/module/port
3. ipv6 dhcp guard [attach-policy policy_name [ vlan {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all } ] | vlan [ {vlan_ids | add vlan_ids | exceptvlan_ids | none | remove vlan_ids | all } ]]
4. do show running-config interface Interface_type stack/module/port
## 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>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 an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td>interface Interface_type stack/module/port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# interface gigabitethernet 1/1/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Attaches the DHCP Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the <strong>attach-policy</strong> option is not used.</td>
</tr>
<tr>
<td>ipv6 dhcp guard [attach-policy policy_name [ vlan vlan_ids</td>
<td>add vlan_ids</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 dhcp guard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# ipv6 dhcp guard vlan 222,223,224</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Confirms that the policy is attached to the specified interface without exiting the configuration mode.</td>
</tr>
<tr>
<td>do show running-config interface Interface_type stack/module/port</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch#(config-if)# do show running-config gig 1/1/4</td>
<td></td>
</tr>
</tbody>
</table>

## How to Attach an IPv6 DHCP Guard Policy to a Layer 2 EtherChannel Interface

Beginning in privileged EXEC mode, follow these steps to attach an IPv6 DHCP Guard policy on an EtherChannel interface or VLAN:

### SUMMARY STEPS

1. configure terminal
2. interface range Interface_name
3. ipv6 dhcp guard [attach-policy policy_name [ vlan vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all ] ] | vlan [ vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all ] ]
### How to Configure IPv6 Source Guard

#### 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>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface range Interface_name</td>
<td>Specify the port-channel interface name assigned when the EtherChannel was created. Enters the interface range configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface Po11</td>
<td></td>
</tr>
</tbody>
</table>

**Tip** Enter the `do show interfaces summary` command for quick reference to interface names and types.

| Step 3 | ipv6 dhcp guard [attach-policy policy_name [ vlan vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all ] ] | Attaches the DHCP Guard policy to the interface or the specified VLANs on that interface. The default policy is attached if the `attach-policy` option is not used. |
| Example: | Switch(config-if-range)# ipv6 dhcp guard attach-policy example_policy | |
| or | Switch(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224 | |
| or | Switch(config-if-range)#ipv6 dhcp guard vlan 222,223,224 | |

| Step 4 | do show running-config interfaceportchannel_interface_name | Confirms that the policy is attached to the specified interface without exiting the configuration mode. |
| Example: | Switch#(config-if-range)# do show running-config int poll | |

### How to Configure IPv6 Source Guard

#### SUMMARY STEPS

1. enable
2. configure terminal
### 3. [no] ipv6 source-guard policy policy_name
4. [deny global-autoconf] [permit link-local] [default{...}] [exit] [no{...}]
5. end
6. show ipv6 source-guard policy policy_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>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></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><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>[no] ipv6 source-guard policy policy_name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# ipv6 source-guard policy example_policy</td>
</tr>
<tr>
<td></td>
<td>Specifies the IPv6 Source Guard policy name and enters IPv6 Source Guard policy configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>[deny global-autoconf] [permit link-local] [default{...}] [exit] [no{...}]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-sisf-sourceguard)# deny global-autoconf</td>
</tr>
<tr>
<td></td>
<td>(Optional) Defines the IPv6 Source Guard policy.</td>
</tr>
<tr>
<td></td>
<td>• deny global-autoconf—Denies data traffic from auto-configured global addresses. This is useful when all global addresses on a link are DHCP-assigned and the administrator wants to block hosts with self-configured addresses to send traffic.</td>
</tr>
<tr>
<td></td>
<td>• permit link-local—Allows all data traffic that is sourced by a link-local address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Trusted option under source guard policy is not supported.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config-sisf-sourceguard)# end</td>
</tr>
<tr>
<td></td>
<td>Exits out of IPv6 Source Guard policy configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show ipv6 source-guard policy policy_name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# show ipv6 source-guard policy example_policy</td>
</tr>
<tr>
<td></td>
<td>Shows the policy configuration and all the interfaces where the policy is applied.</td>
</tr>
</tbody>
</table>

**What to do next**

Apply the IPv6 Source Guard policy to an interface.
How to Attach an IPv6 Source Guard Policy to an Interface

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface` `Interface_type stack/module/port`
4. `ipv6 source-guard` `[attach-policy <policy_name>]`
5. `show ipv6 source-guard policy policy_name`

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 the 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>interface</code> <code>Interface_type stack/module/port</code></td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config)# interface gigabitethernet 1/1/4</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ipv6 source-guard</code> <code>[attach-policy &lt;policy_name&gt;]</code></td>
<td>Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the <code>attach-policy</code> option is not used.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch(config-if)# ipv6 source-guard attach-policy example_policy</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>show ipv6 source-guard policy policy_name</code></td>
<td>Shows the policy configuration and all the interfaces where the policy is applied.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>Switch#(config-if)# show ipv6 source-guard policy example_policy</code></td>
<td></td>
</tr>
</tbody>
</table>

How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface port-channel port-channel-number`
4. ipv6 source-guard [attach-policy <policy_name>]  
5. show ipv6 source-guard policy policy_name

**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 the global configuration mode.  
  Example:  
  Switch# configure terminal |
| **Step 3** interface port-channel port-channel-number | Specifies an interface type and port number and places the switch in the port channel configuration mode.  
  Example:  
  Switch (config)# interface Po4 |
| **Step 4** ipv6 source-guard [attach-policy <policy_name>] | Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the attach-policy option is not used.  
  Example:  
  Switch(config-if)# ipv6 source-guard attach-policy example_policy |
| **Step 5** show ipv6 source-guard policy policy_name | Shows the policy configuration and all the interfaces where the policy is applied.  
  Example:  
  Switch(config-if)# show ipv6 source-guard policy example_policy |

**How to Configure IPv6 Prefix Guard**

**Note**

To allow routing protocol control packets sourced by a link-local address when prefix guard is applied, enable the permit link-local command in the source-guard policy configuration mode.

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. [no] ipv6 source-guard policy source-guard-policy  
4. [no] validate address  
5. validate prefix  
6. exit
### 7. show ipv6 source-guard policy [source-guard-policy]

#### 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> [no] ipv6 source-guard policy source-guard-policy</td>
<td>Defines an IPv6 source-guard policy name and enters switch integrated security features source-guard policy configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config)# ipv6 source-guard policy my_snooping_policy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> [ no ] validate address</td>
<td>Disables the validate address feature and enables the IPv6 prefix guard feature to be configured.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-sisf-sourceguard)# no validate address</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> validate prefix</td>
<td>Enables IPv6 source guard to perform the IPv6 prefix-guard operation.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-sisf-sourceguard)# validate prefix</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits switch integrated security features source-guard policy configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch (config-sisf-sourceguard)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show ipv6 source-guard policy [source-guard-policy]</td>
<td>Displays the IPv6 source-guard policy configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch # show ipv6 source-guard policy policy1</td>
<td></td>
</tr>
</tbody>
</table>

### How to Attach an IPv6 Prefix Guard Policy to an Interface

#### SUMMARY STEPS

1. enable
2. configure terminal
3. interface Interface_type stack/module/port
4. ipv6 source-guard attach-policy policy_name
5. `show ipv6 source-guard policy policy_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: Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface Interface_type stack/module/port</td>
<td>Specifies an interface type and identifier; enters the interface configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# interface gigabitethernet 1/1/4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 source-guard attach-policy policy_name</td>
<td>Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the attach-policy option is not used.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# ipv6 source-guard attach-policy example_policy</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show ipv6 source-guard policy policy_name</td>
<td>Shows the policy configuration and all the interfaces where the policy is applied.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# show ipv6 source-guard policy example_policy</td>
<td></td>
</tr>
</tbody>
</table>

**How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface port-channel port-channel-number
4. ipv6 source-guard [attach-policy <policy_name> ]
5. show ipv6 source-guard policy policy_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>
</tbody>
</table>
### Purpose

<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:**

```plaintext
Switch# configure terminal
```

Enters the global configuration mode.

#### Step 3

**interface port-channel port-channel-number**

**Example:**

```plaintext
Switch (config)# interface Po4
```

Specifies an interface type and port number and places the switch in the port channel configuration mode.

#### Step 4

**ipv6 source-guard [attach-policy <policy_name>]**

**Example:**

```plaintext
Switch(config-if)# ipv6 source-guard attach-policy example_policy
```

Attaches the IPv6 Source Guard policy to the interface. The default policy is attached if the `attach-policy` option is not used.

#### Step 5

**show ipv6 source-guard policy policy_name**

**Example:**

```plaintext
Switch(config-if)# show ipv6 source-guard policy example_policy
```

Shows the policy configuration and all the interfaces where the policy is applied.

---

### Configuration Examples for IPv6 First Hop Security

#### Examples: How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface

The following example shows how to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface:

```plaintext
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch(config-sisf-sourceguard)# validate address
Switch(config-sisf-sourceguard)# exit
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config)# ipv6 source-guard attach-policy POL
Switch(config)# exit
switch(config)#
```

#### Examples: How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface

The following example shows how to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface:

```plaintext
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch (config-sisf-sourceguard)# no validate address
```
Switch(config-sisf-sourceguard)# validate prefix
Switch(config)# interface Po4
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL

**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>

**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>
CHAPTER 48

Per-User ACL Support for 802.1X/MAB/Webauth Users

This feature allows per-user ACLs to be downloaded from the Cisco Access Control Server (ACS) as policy enforcement after authentication using IEEE 802.1X, MAB authentication bypass, or web authentication.

- Finding Feature Information, on page 921
- Prerequisites for Per-User ACL Support for 802.1X/MAB/Webauth Users, on page 921
- Restrictions for Per-User ACL Support for 802.1X/MAB/Webauth Users, on page 922
- Information About Per-User ACL Support for 802.1X/MAB/Webauth Users, on page 922
- How to Configure Per-User ACL Support for 802.1X/MAB/Webauth Users, on page 923
- Configuration Examples for Per-User ACL Support for 802.1X/MAB/Webauth Users, on page 924
- Additional References, on page 925
- Feature Information for Per-User ACL Support for 802.1X/MAB/Webauth Users, on page 926

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 Per-User ACL Support for 802.1X/MAB/Webauth Users

- AAA authentication must be enabled.
- AAA authorization must be enabled by using the network keyword to allow interface configuration from the RADIUS server.
- 802.1X authentication must be enabled.
- The user profile and VSAs must be configured on the RADIUS server.
Restrictions for Per-User ACL Support for 802.1X/MAB/Webauth Users

- Per-user Access Control Lists (ACLs) are supported only in single-host mode.
- This feature does not support standard ACLs on the switch port.
- Only one 802.1X-authenticated user is supported on a port. If the multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.
- The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

Information About Per-User ACL Support for 802.1X/MAB/Webauth Users

802.1X Authentication with Per-User ACLs

Per-user access control lists (ACLs) can be configured to provide different levels of network access and service to an 802.1X-authenticated user. When the RADIUS server authenticates a user that is connected to an 802.1X port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1X port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are in acl#<n> for the ingress direction and outacl#<n> for the egress direction. MAB ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It does not support port ACLs in the egress direction on Layer 2 ports. For more information, see the “Configuring Network Security with ACLs” module.

The extended ACL syntax style should be used to define the per-user configuration that is stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if the Filter-Id attribute is used, it can point to a standard ACL.

The Filter-Id attribute can be used to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by .in for ingress filtering or .out for egress filtering. If the RADIUS server does not allow the .in or .out syntax, the access list is applied to the outbound ACL by default. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and IP extended ACLs).

Only one 802.1X-authenticated user is supported on a port. If the multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.
# How to Configure Per-User ACL Support for 802.1X/MAB/Webauth Users

## Configuring Downloadable ACLs

To configure a switch to accept downloadable ACLs or redirect URLs from the RADIUS server during authentication of an attached host, perform this task.

### SUMMARY STEPS

1. enable
2. configure terminal
3. ip device tracking
4. aaa new-model
5. aaa authorization network default group radius
6. radius-server vsa send authentication
7. interface interface-id
8. ip access-group acl-id in
9. end
10. show running-config interface interface-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><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> ip device tracking</td>
<td>Enables the IP device tracking table.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# ip device tracking</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config)# aaa new-model</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 5**

`aaa authorization network default group radius`

**Example:**

Switch(config)# aaa authorization network default group radius

**Purpose:**

Sets the authorization method. To remove the authorization method, use the `no aaa authorization network default group radius` command.

**Step 6**

`radius-server vsa send authentication`

**Example:**

Switch(config)# radius-server vsa send authentication

**Purpose:**

Configures the network access server.

**Step 7**

`interface interface-id`

**Example:**

Switch(config)# interface gigabitethernet0/1

**Purpose:**

Specifies the port to be configured, and enters interface configuration mode.

**Step 8**

`ip access-group acl-id in`

**Example:**

Switch(config-if)# ip access-group 99 in

**Note**

The ACL ID is an access list name or number.

**Step 9**

`end`

**Example:**

Switch(config-if)# end

**Purpose:**

Returns to Privileged EXEC mode.

**Step 10**

`show running-config interface interface-id`

**Example:**

Switch# show running-config interface interface-id

**Purpose:**

Displays the specific interface configuration for verification.

**Step 11**

`copy running-config startup-config`

**Example:**

Switch# copy running-config startup-config

**Purpose:**

(Optional) Save entries in the configuration file.

---

### Configuration Examples for Per-User ACL Support for 802.1X/MAB/Webauth Users

#### Example: Configuring a Switch for a Downloadable Policy

The following example shows how to configure a switch for a downloadable policy:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
```
Switch(config-ext-nacl)## permit ip any any
Switch(config-ext-nacl)## exit
Switch(config)## radius-server vsa send authentication
Switch(config)## interface fastEthernet 2/13
Switch(config-if)## ip access-group default_acl in
Switch(config-if)## exit

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication commands</td>
<td>Cisco IOS Security Command Reference Commands A to C</td>
</tr>
<tr>
<td>RADIUS</td>
<td>“Configuring RADIUS” module.</td>
</tr>
<tr>
<td>Standalone MAB Support</td>
<td>Standalone MAB Support</td>
</tr>
<tr>
<td>Layer 2 ports</td>
<td>Configuring Network Security with ACLs</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.1X protocol</td>
<td>—</td>
</tr>
<tr>
<td>RFC 3580</td>
<td>IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)</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 releases,</td>
</tr>
<tr>
<td>• CISCO-MAB-AUTH-BYPASS-MIB</td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td>• CISCO-PAE-MIB</td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• IEEE8021-PAE-MIB</td>
<td></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 Per-User ACL Support for 802.1X/MAB/Webauth Users

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 99: Feature Information for Per-User ACL Support for 802.1X/MAB/Webauth Users

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-User ACL Support for 802.1X/MAB/Webauth Users</td>
<td></td>
<td>This feature allows per-user ACLs to be downloaded from the Cisco Access Control Server (ACS) as policy enforcement after authentication using IEEE 802.1X, MAB authentication bypass, or web authentication.</td>
</tr>
</tbody>
</table>
CHAPTER 49

Web Authentication Redirection to Original URL

The Web Authentication Redirection to Original URL feature enables networks to redirect guest users to the URL that they had originally requested. This feature is enabled by default and requires no configuration. This module provides information about this feature.

- Web Authentication Redirection to Original URL Overview, on page 927

Web Authentication Redirection to Original URL Overview

The Web Authentication Redirection to Original URL feature enables networks to redirect guest users to the URL that they had originally requested. This feature is enabled by default and requires no configuration.

Guest networks are network connections provided by an enterprise to allow their guests to gain access to the Internet and to their own enterprise networks without compromising the security of the host enterprise. Guest users of an enterprise network can connect to the guest access network through either a wired Ethernet connection or a wireless connection.

Guest access uses a captive portal to gather all web requests made by guests and redirect these requests to one of the guest on-boarding web pages. When guests successfully complete the guest workflow, they are redirected to the page that they had originally requested.

The originally requested URL is passed as metadata along with the Cisco Identity Services Engine (ISE) guest access redirect URL. The Cisco ISE is a security policy management and control platform. It automates and simplifies access control and security compliance for wired, wireless, and VPN connectivity. The requested URL is added at the end of the Cisco ISE guest URL so that the device can send the redirect URL to the guest client. The Cisco ISE parses the URL and redirects the guest to the original URL after completing the on-boarding.

The following is an example of a redirect URL along with the original requested URL:


In this example, the URL, https://10.64.67.92:8443/guestportal/gateway?sessionId=0920269E0000000B0002426B&action=cwa is the URL for the guest portal, “&” tells the browser that what follows is a list of name value pairs, and redirect_url=http://www.cisco.com identifies the URL that the user originally requested and to which the user is redirected after completing the guest workflow.

This illustration displays the packet flow that redirects a user to the originally requested URL:
1. A user accesses a network for the first time and sends an HTTP request to access www.google.com. When the user first accesses the network, a MAC authentication bypass (MAB) is triggered and the MAC address is sent to the Cisco ISE.

2. The Cisco ISE returns a RADIUS access-accept message (even if the MAC address is not received) along with the redirect access control list (ACL), the ACL-WEBAUTH-REDIRECT message, and the guest web portal URL to the device.

The RADIUS message instructs the device to open a port that is restricted based on the configured port and the redirect ACLs, for regular network traffic.
3. When the user launches a web browser, the device intercepts the HTTP traffic and redirects the browser to the Cisco ISE central web authentication (CWA) guest web portal URL; the user-requested URL is extracted and appended to the Cisco ISE guest URL.

4. When the user is authenticated, the Cisco ISE sends the Device Registration page to the user. The user enters the required information, and the page is returned to the Cisco ISE. The Cisco ISE downloads user profiles and redirects the user to the originally requested URL: www.google.com.

Additional References for Web Authentication Redirection to Original URL

### 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>IBNS commands</td>
<td>Cisco IOS Identity-Based Networking Services Command Reference</td>
</tr>
<tr>
<td>Wired guest access</td>
<td>“Wired Guest Access” module of the Identity-Based Networking Services Configuration Guide</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 Web Authentication Redirection to Original URL

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Authentication Redirection to Original URL</td>
<td>Cisco IOS Release 15.2(6)E</td>
<td>The Web Authentication Redirection to Original URL feature enables networks to redirect guest users to the original URL that they had request. This feature is enabled by default and requires no configuration. In</td>
</tr>
</tbody>
</table>
Configuring Web-Based Authentication

The Web-Based Authentication feature, also known as web authentication proxy, authenticates end users on host systems that do not run the IEEE 802.1x supplicant.

- Finding Feature Information, on page 931
- Restrictions for Web-Based Authentication, on page 931
- Information About Web-Based Authentication, on page 931
- How to Configure Web-Based Authentication, on page 945
- Configuration Examples for Web-Based Authentication, on page 956
- Additional References for Web-Based Authentication, on page 958
- Feature Information for Web-Based Authentication, on page 959

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 Web-Based Authentication

- Web-based authentication and url-redirect are not supported on the same port at the same time.

Information About Web-Based Authentication

Web-Based Authentication Overview

Use the web-based authentication feature, known as web authentication proxy, to authenticate end users on host systems that do not run the IEEE 802.1x supplicant.
You can configure web-based authentication on Layer 2 interfaces only.

When you initiate an HTTP session, web-based authentication intercepts ingress HTTP packets from the host and sends an HTML login page to the users. The users enter their credentials, which the web-based authentication feature sends to the authentication, authorization, and accounting (AAA) server for authentication.

If authentication succeeds, web-based authentication sends a Login-Successful HTML page to the host and applies the access policies returned by the AAA server.

If authentication fails, web-based authentication forwards a Login-Fail HTML page to the user, prompting the user to retry the login. If the user exceeds the maximum number of attempts, web-based authentication forwards a Login-Expired HTML page to the host, and the user is placed on a watch list for a waiting period.

HTTPS traffic interception for central web authentication redirect is not supported.

You should use global parameter-map (for method-type, custom, and redirect) only for using the same web authentication methods like consent, web consent, and webauth, for all the clients and SSIDs. This ensures that all the clients have the same web-authentication method.

If the requirement is to use Consent for one SSID and Web-authentication for another SSID, then you should use two named parameter-maps. You should configure Consent in first parameter-map and configure webauth in second parameter-map.

Based on where the web pages are hosted, the local web authentication can be categorized as follows:

- **Internal**—The internal default HTML pages (Login, Success, Fail, and Expire) in the controller are used during the local web authentication.
- **Customized**—The customized web pages (Login, Success, Fail, and Expire) are downloaded onto the controller and used during the local web authentication.
- **External**—The customized web pages are hosted on the external web server instead of using the in-built or custom web pages.

Based on the various web authentication pages, the types of web authentication are as follows:

- **Webauth**—This is a basic web authentication. Herein, the controller presents a policy page with the user name and password. You need to enter the correct credentials to access the network.

- **Consent or web-passthrough**—Herein, the controller presents a policy page with the Accept or Deny buttons. You need to click the Accept button to access the network.

- **Webconsent**—This is a combination of webauth and consent web authentication types. Herein, the controller presents a policy page with Accept or Deny buttons along with user name or password. You need to enter the correct credentials and click the Accept button to access the network.
Device Roles

With web-based authentication, the devices in the network have these specific roles:

- **Client**—The device (workstation) that requests access to the LAN and the services and responds to requests from the switch. The workstation must be running an HTML browser with JavaScript enabled.

- **Authentication server**—Authenticates the client. The authentication server validates the identity of the client and notifies the switch that the client is authorized to access the LAN and the switch services or that the client is denied.

- **Switch**—Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client.

*Figure 66: Web-Based Authentication Device Roles*

This figure shows the roles of these devices in a network.

Host Detection

The switch maintains an IP device tracking table to store information about detected hosts.

For Layer 2 interfaces, web-based authentication detects IP hosts by using these mechanisms:

- **ARP based trigger**—ARP redirect ACL allows web-based authentication to detect hosts with a static IP address or a dynamic IP address.
- **Dynamic ARP inspection**
- **DHCP snooping**—Web-based authentication is notified when the switch creates a DHCP-binding entry for the host.

Session Creation

When web-based authentication detects a new host, it creates a session as follows:

- Reviews the exception list.

  If the host IP is included in the exception list, the policy from the exception list entry is applied, and the session is established.

- Reviews for authorization bypass.
If the host IP is not on the exception list, web-based authentication sends a nonresponsive-host (NRH) request to the server.

If the server response is access accepted, authorization is bypassed for this host. The session is established.

- Sets up the HTTP intercept ACL

If the server response to the NRH request is access rejected, the HTTP intercept ACL is activated, and the session waits for HTTP traffic from the host.

**Authentication Process**

When you enable web-based authentication, these events occur:

- The user initiates an HTTP session.

- The HTTP traffic is intercepted, and authorization is initiated. The switch sends the login page to the user. The user enters a username and password, and the switch sends the entries to the authentication server.

- If the authentication succeeds, the switch downloads and activates the user’s access policy from the authentication server. The login success page is sent to the user.

- If the authentication fails, the switch sends the login fail page. The user retries the login. If the maximum number of attempts fails, the switch sends the login expired page, and the host is placed in a watch list. After the watch list times out, the user can retry the authentication process.

- If the authentication server does not respond to the switch, and if an AAA fail policy is configured, the switch applies the failure access policy to the host. The login success page is sent to the user.

- The switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface.

- The feature applies the downloaded timeout or the locally configured session timeout.

- If the terminate action is RADIUS, the feature sends a nonresponsive host (NRH) request to the server. The terminate action is included in the response from the server.

- If the terminate action is default, the session is dismantled, and the applied policy is removed.

**Using Authentication Proxy**

The authentication proxy feature requires some user interaction on the client host. The table below describes the interaction of the authentication proxy with the client host.

<table>
<thead>
<tr>
<th>Authentication Proxy Action with Client</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggering on HTTP connections</td>
<td>If a user is not currently authenticated at the firewall router, any HTTP connection initiated by the user triggers the authentication proxy. If the user is already authenticated, the authentication proxy is transparent to the user.</td>
</tr>
</tbody>
</table>
### When to Use the Authentication Proxy

The following are some situations in which you can use the authentication proxy:

- You want to manage access privileges on an individual (per-user) basis using the services provided by the authentication servers instead of configuring access control based on host IP address or global access policies. Authenticating and authorizing users from any host IP address also allows network administrators to configure host IP addresses using DHCP.

- You want to authenticate and authorize local users before permitting access to intranet or Internet services.

- You want to authenticate and authorize remote users before permitting access to local services.

- You want to control access for specific extranet users. For example, you might want to authenticate and authorize the financial officer of a corporate partner with one set of access privileges while authorizing the technology officer for that same partner to use another set of access privileges.

- You want to use the authentication proxy in conjunction with VPN client software to validate users and to assign specific access privileges.

- You want to use the authentication proxy in conjunction with AAA accounting to generate “start” and “stop” accounting records that can be used for billing, security, or resource allocation purposes, thereby allowing users to track traffic from the authenticated hosts.

### Applying Authentication Proxy

Apply the authentication proxy in the inbound direction at any interface on the router where you want per-user authentication and authorization. Applying the authentication proxy inbound at an interface causes it to intercept the initial connection request from an user, before that request is subjected to any other processing. If the user fails to gain authentication with the AAA server, the connection request is dropped.
How you apply the authentication proxy depends on your security policy. For example, you can block all traffic through an interface and enable the authentication proxy feature to require authentication and authorization for all user-initiated HTTP connections. Users are authorized for services only after successful authentication with the AAA server.

The authentication proxy feature also allows you to use standard access lists to specify a host or group of hosts whose initial HTTP traffic triggers the proxy.

The figure below shows the authentication proxy applied at the LAN interface with all network users required to be authenticated upon the initial connection (all traffic is blocked at each interface).

**Figure 67: Applying the Authentication Proxy at the Local Interface**

The figure below shows the authentication proxy applied at the dial-in interface with all network traffic blocked at each interface.

**Figure 68: Applying the Authentication Proxy at an Outside Interface**

**Local Web Authentication Banner**

With Web Authentication, you can create a default and customized web-browser banners that appears when you log in to a switch.

The banner appears on both the login page and the authentication-result pop-up pages. The default banner messages are as follows:

- **Authentication Successful**
- **Authentication Failed**
- **Authentication Expired**

The Local Web Authentication Banner can be configured in legacy and new-style (Session-aware) CLIs as follows:
• Legacy mode—Use the `ip admission auth-proxy-banner http` global configuration command.

• New-style mode—Use the `parameter-map type webauth global banner` global configuration command.

The default banner Cisco Systems and Switch host-name Authentication appear on the Login Page. Cisco Systems appears on the authentication result pop-up page.

*Figure 69: Authentication Successful Banner*

The banner can be customized as follows:

• Add a message, such as switch, router, or company name to the banner:
  - Legacy mode—Use the `ip admission auth-proxy-banner http banner-text` global configuration command.
  - New-style mode—Use the `parameter-map type webauth global banner` global configuration command.

• Add a logo or text file to the banner:
  - Legacy mode—Use the `ip admission auth-proxy-banner http file-path` global configuration command.
  - New-style mode—Use the `parameter-map type webauth global banner` global configuration command.
If you do not enable a banner, only the username and password dialog boxes appear in the web authentication login screen, and no banner appears when you log into the switch.
Web Authentication Customizable Web Pages

During the web-based authentication process, the switch internal HTTP server hosts four HTML pages to deliver to an authenticating client. The server uses these pages to notify you of these four-authentication process states:

- **Login**—Your credentials are requested.
- **Success**—The login was successful.
- **Fail**—The login failed.
- **Expire**—The login session has expired because of excessive login failures.

**Guidelines**

- You can substitute your own HTML pages for the default internal HTML pages.
- You can use a logo or specify text in the `login`, `success`, `failure`, and `expire` web pages.
- On the banner page, you can specify text in the login page.
- The pages are in HTML.
- You must include an HTML redirect command in the success page to access a specific URL.
- The URL string must be a valid URL (for example, http://www.cisco.com). An incomplete URL might cause *page not found* or similar errors on a web browser.
- If you configure web pages for HTTP authentication, they must include the appropriate HTML commands (for example, to set the page time out, to set a hidden password, or to confirm that the same page is not submitted twice).
- The CLI command to redirect users to a specific URL is not available when the configured login form is enabled. The administrator should ensure that the redirection is configured in the web page.
- If the CLI command redirecting users to specific URL after authentication occurs is entered and then the command configuring web pages is entered, the CLI command redirecting users to a specific URL does not take effect.
- Configured web pages can be copied to the switch boot flash or flash.
- The login page can be on one flash, and the success and failure pages can be another flash.
- You must configure all four pages.
- The banner page has no effect if it is configured with the web page.
- All of the logo files (image, flash, audio, video, and so on) that are stored in the system directory (for example, flash, disk0, or disk) and that must be displayed on the login page must use `web_auth_<filename>` as the file name.
- The configured authentication proxy feature supports both HTTP and SSL.

You can substitute your HTML pages for the default internal HTML pages. You can also specify a URL to which users are redirected after authentication occurs, which replaces the internal Success page.
Authentication Proxy Web Page Guidelines

When configuring customized authentication proxy web pages, follow these guidelines:

- To enable the custom web pages feature, specify all four custom HTML files. If you specify fewer than four files, the internal default HTML pages are used.

- The four custom HTML files must be present on the flash memory of the switch. The maximum size of each HTML file is 8 KB.

- Any images on the custom pages must be on an accessible HTTP server. Configure an intercept ACL within the admission rule.

- Any external link from a custom page requires configuration of an intercept ACL within the admission rule.

- To access a valid DNS server, any name resolution required for external links or images requires configuration of an intercept ACL within the admission rule.

- If the custom web pages feature is enabled, a configured auth-proxy-banner is not used.

- If the custom web pages feature is enabled, the redirection URL for successful login feature is not available.

- To remove the specification of a custom file, use the `no` form of the command.

Because the custom login page is a public web form, consider these guidelines for the page:

- The login form must accept user entries for the username and password and must show them as `uname` and `pwd`.

- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.
Web-based Authentication Interactions with Other Features

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.

- Cisco IOS Release 12.2(55)SE and later supports filtering of system messages related to 802.1x authentication.

AAA Accounting with Authentication Proxy

Using the authentication proxy, you can generate “start” and “stop” accounting records with enough information to be used for billing and security auditing purposes. Thus, you can monitor the actions of authenticated hosts that use the authentication proxy service.

When an authentication proxy cache expires and is deleted, additional data, such as elapsed time, is added to the accounting information and a “stop” record is sent to the server. At this point, the information is deleted from the data structure.

The accounting records for the authentication proxy user session are related to the cache and the dynamic ACL usage.
ACLs

You must configure port ACLs on interfaces for web-based authentication. Ensure that sufficient TCAM space is available to enable web-based authentication.

If you configure a VLAN ACL or a Cisco IOS ACL on an interface, the ACL is applied to the host traffic only after the web-based authentication host policy is applied.

For Layer 2 web-based authentication, it is more secure, though not required, to configure a port ACL (PACL) as the default access policy for ingress traffic from hosts connected to the port. After authentication, the web-based authentication host policy overrides the PACL. The Policy ACL is applied to the session even if there is no ACL configured on the port.

You cannot configure a MAC ACL and web-based authentication on the same interface.

You cannot configure web-based authentication on a port whose access VLAN is configured for VACL capture.

Context-Based Access Control

Web-based authentication cannot be configured on a Layer 2 port if context-based access control (CBAC) is configured on the Layer 3 VLAN interface of the port VLAN.

Gateway IP

You cannot configure Gateway IP (GWIP) on a Layer 3 VLAN interface if web-based authentication is configured on any of the switch ports in the VLAN.

You can configure web-based authentication on the same Layer 3 interface as Gateway IP. The host policies for both features are applied in software. The GWIP policy overrides the web-based authentication host policy.

LAN Port IP

You can configure LAN port IP (LPIP) and Layer 2 web-based authentication on the same port. The host is authenticated by using web-based authentication first, followed by LPIP posture validation. The LPIP host policy overrides the web-based authentication host policy.

If the web-based authentication idle timer expires, the NAC policy is removed. The host is authenticated, and posture is validated again.

Port Security

You can configure web-based authentication and port security on the same port. Web-based authentication authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through the port.

Default Web-Based Authentication Configuration

The following table shows the default web-based authentication configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
**Web-Based Authentication Configuration Guidelines and Restrictions**

- Web-based authentication is an ingress-only feature.
- You can configure web-based authentication only on access ports. Web-based authentication is not supported on trunk ports, EtherChannel member ports, or dynamic trunk ports.
- Port ACLs must be present in the port configuration. If they are not present, adding intercept ACL will fail.
- Port ACLs should be configured sufficiently to allow the necessary traffic after authentication.
- The switch supports one web authentication client per port on all host modes. Having multiple clients may lead to unexpected results and is not recommended.
- Configuring port ACLs in the authentication rule for web authentication is not allowed because DACL is not supported.
- You cannot authenticate hosts on Layer 2 interfaces with static ARP cache assignment. These hosts are not detected by the web-based authentication feature because they do not send ARP messages.
- By default, the IP device tracking feature is disabled on a switch. You must enable the IP device tracking feature to use web-based authentication.
- You must configure at least one IP address to run the switch HTTP server. You must also configure routes to reach each host IP address. The HTTP server sends the HTTP login page to the host.
- Hosts that are more than one hop away might experience traffic disruption if an STP topology change results in the host traffic arriving on a different port. This occurs because the ARP and DHCP updates might not be sent after a Layer 2 (STP) topology change.
- Web-based authentication does not support VLAN assignment as a downloadable-host policy.
- Web-based authentication and Network Edge Access Topology (NEAT) are mutually exclusive. You cannot use web-based authentication when NEAT is enabled on an interface, and you cannot use NEAT when web-based authentication is running on an interface.
- Web-based authentication NRH (Non-Responsive Host) is not supported for voice devices.
- Only the Password Authentication Protocol (PAP) is supported for web-based RADIUS authentication on controllers. The Challenge Handshake Authentication Protocol (CHAP) is not supported for web-based RADIUS authentication on controllers.
• Identify the following RADIUS security server settings that will be used while configuring switch-to-RADIUS-server communication:
  • Host name
  • Host IP address
  • Host name and specific UDP port numbers
  • IP address and specific UDP port numbers

The combination of the IP address and UDP port number creates a unique identifier, that 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, authentication) the second host entry that is configured functions as the failover backup to the first one. The RADIUS host entries are chosen in the order that they were configured.

• When you configure the RADIUS server parameters:
  • Specify the key string on a separate command line.
  • 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.
  • When you specify the key string, use spaces within and at the end of the key. 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 globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using with the radius-server host global configuration command. If you want to configure these options on a per-server basis, use the radius-server timeout, radius-server transmit, and the radius-server key global configuration commands.

Note
You need to configure some settings on the RADIUS server, including: the switch IP address, the key string to be shared by both the server and the switch, and the downloadable ACL (DACL). For more information, see the RADIUS server documentation.

• You cannot start a web-based authentication session from a PC connected to an IP phone in MDA/MA mode (because downloadable ACLs are not supported).

• The switch cannot be configured as gateway for web-based authentication clients (because there is no Layer 3 lookup happening on the switch). Instead, configure an uplink device switch virtual interface (SVI) as gateway.

• The total TCAM space according to the ASIC is limited to 384. So if port ACLs and Web-based authentication is configured across all the ports, the total number of sessions will depend on the access control entries (ACE) that have been configured on the switch. (Ports configured with web-based authentication will not share ACLs in the TCAM. Once the TCAM space is full with port ACLs, web-based authentication sessions will not start.)
# How to Configure Web-Based Authentication

## Configuring the Authentication Rule and Interfaces

Follow these steps to configure the authentication rule and interfaces:

### SUMMARY 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></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>3.</td>
<td><code>ip admission name name proxy http</code></td>
<td>Configures an authentication rule for web-based authorization.</td>
</tr>
<tr>
<td>4.</td>
<td><code>interface type slot/port</code></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td><code>ip access-group name</code></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td><code>ip admission name</code></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td><code>exit</code></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td><code>ip device tracking</code></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td><code>show ip admission</code></td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### 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>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>ip admission name name proxy http</code></td>
<td>Configures an authentication rule for web-based authorization.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# ip admission name webauth1 proxy http</code></td>
<td></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>4</td>
<td><code>interface type slot/port</code></td>
<td>Enters interface configuration mode and specifies the ingress Layer 2 or Layer 3 interface to be enabled for web-based authentication. <code>type</code> can be fastethernet, gigabit ethernet, or tengigabitethernet.</td>
</tr>
<tr>
<td>5</td>
<td><code>ip access-group name</code></td>
<td>Applies the default ACL.</td>
</tr>
<tr>
<td>6</td>
<td><code>ip admission name</code></td>
<td>Configures an authentication rule for web-based authorization for the interface.</td>
</tr>
<tr>
<td>7</td>
<td><code>exit</code></td>
<td>Returns to configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td><code>ip device tracking</code></td>
<td>Enables the IP device tracking table.</td>
</tr>
<tr>
<td>9</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>10</td>
<td><code>show ip admission</code></td>
<td>Displays the configuration.</td>
</tr>
<tr>
<td>11</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
# Configuring AAA Authentication

## SUMMARY STEPS

1. `aaa new-model`
2. `aaa authentication login default group {tacacs+ | radius}`
3. `aaa authorization auth-proxy default group {tacacs+ | radius}`
4. `tacacs-server host {hostname | ip_address}`
5. `tacacs-server key {key-data}`

## 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 AAA functionality.</td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# aaa new-model</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Defines the list of authentication methods at login.</td>
</tr>
<tr>
<td>`aaa authentication login default group {tacacs+</td>
<td>radius}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# aaa authentication login default group tacacs+</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Creates an authorization method list for web-based authorization.</td>
</tr>
<tr>
<td>`aaa authorization auth-proxy default group {tacacs+</td>
<td>radius}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# aaa authorization auth-proxy default group tacacs+</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Specifies an AAA server.</td>
</tr>
<tr>
<td>`tacacs-server host {hostname</td>
<td>ip_address}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# tacacs-server host 10.1.1.1</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the authorization and encryption key used between the switch and the TACACS server.</td>
</tr>
<tr>
<td><code>tacacs-server key {key-data}</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Switch(config)# tacacs-server key</code></td>
</tr>
</tbody>
</table>
Configuring Switch-to-RADIUS-Server Communication

Follow these steps to configure the RADIUS server parameters:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip radius source-interface
4. radius-server host {hostname | ip-address} test username username
5. radius-server key string
6. radius-server dead-criteria tries num-tries
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>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> ip radius source-interface</td>
<td>Specifies that the RADIUS packets have the IP address of the indicated interface.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip radius source-interface vlan 80</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> radius-server host {hostname</td>
<td>ip-address} test username username</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server host 172.120.39.46 test username user1</td>
<td>The test username username option enables automated testing of the RADIUS server connection. The specified username does not need to be a valid user name.</td>
</tr>
<tr>
<td></td>
<td>The key option specifies an authentication and encryption key to use between the switch and the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>To use multiple RADIUS servers, reenter this command for each server.</td>
</tr>
</tbody>
</table>
### Purpose

Configure the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.

**Command or Action**  
```
radius-server key string
```

**Example:**
```
Switch(config)# radius-server key rad123
```

### Step 5

Specify the number of unanswered sent messages to a RADIUS server before considering the server to be inactive. The range of `num-tries` is 1 to 100.

**Command or Action**  
```
radius-server dead-criteria tries num-tries
```

**Example:**
```
Switch(config)# radius-server dead-criteria tries 30
```

### Step 6

Return to privileged EXEC mode.

**Command or Action**  
```
end
```

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

### Configuring the HTTP Server

To use web-based authentication, you must enable the HTTP server within the Switch. You can enable the server for either HTTP or HTTPS.

**Note**

The Apple pseudo-browser will not open if you configure only the `ip http secure-server` command. You should also configure the `ip http server` command.

Follow these steps to enable the server for either HTTP or HTTPS:

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. ip http server  
4. ip http secure-server  
5. 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. |

<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. |
### Command or Action

**Step 2**
- **configure terminal**
  - Example:
    ```
    Switch# configure terminal
    ```

  Enters global configuration mode.

**Step 3**
- **ip http server**
  - Example:
    ```
    Switch(config)# ip http server
    ```

  Enables the HTTP server. The web-based authentication feature uses the HTTP server to communicate with the hosts for user authentication.

**Step 4**
- **ip http secure-server**
  - Example:
    ```
    Switch(config)# ip http secure-server
    ```

  Enables HTTPS.

  You can configure custom authentication proxy web pages or specify a redirection URL for successful login.

  **Note** To ensure secure authentication when you enter the `ip http secure-server` command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.

**Step 5**
- **end**
  - Example:
    ```
    Switch(config)# end
    ```

  Returns to privileged EXEC mode.

### Customizing the Authentication Proxy Web Pages

You can configure web authentication to display four substitute HTML pages to the user in place of the Switch default HTML pages during web-based authentication.

Follow these steps to specify the use of your custom authentication proxy web pages:

**Before you begin**
- Store your custom HTML files on the Switch flash memory.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip admission proxy http login page file device:login-filename`
4. `ip admission proxy http success page file device:success-filename`
5. `ip admission proxy http failure page file device:fail-filename`
6. `ip admission proxy http login expired page file device:expired-filename`
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>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> ip admission proxy http login page file device:login-filename</td>
<td>Specifies the location in the Switch memory file system of the custom HTML file to use in place of the default login page. The device: is flash memory.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip admission proxy http login page file disk1:login.htm</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip admission proxy http success page file device:success-filename</td>
<td>Specifies the location of the custom HTML file to use in place of the default login success page.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip admission proxy http success page file disk1:success.htm</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip admission proxy http failure page file device:fail-filename</td>
<td>Specifies the location of the custom HTML file to use in place of the default login failure page.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip admission proxy http fail page file disk1:fail.htm</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ip admission proxy http login expired page file device:expired-filename</td>
<td>Specifies the location of the custom HTML file to use in place of the default login expired page.</td>
</tr>
<tr>
<td>Example: Switch(config)# ip admission proxy http login expired page file disk1:expired.htm</td>
<td></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>
### Configuring the Web-Based Authentication Parameters

Follow these steps to configure the maximum number of failed login attempts before the client is placed in a watch list for a waiting period:

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip admission max-login-attempts number`
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>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch&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></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip admission max-login-attempts number</code></td>
<td>Sets the maximum number of failed login attempts. The range is 1 to 2147483647 attempts. The default is 5.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# ip admission max-login-attempts 10</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:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Web Authentication Local Banner

For the equivalent Session Aware Networking configuration example for this feature, see the section "Configuring a Parameter Map for Web-Based Authentication" in the chapter, "Configuring Identity Control Policies" of the book,"Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)."

Beginning in privileged EXEC mode, follow these steps to configure a local banner on a switch that has web authentication configured.

**SUMMARY STEPS**

1. `configure terminal`
2. `ip auth-proxy auth-proxy-banner http [banner-text | file-path]`
3. `end`
4. `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>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables the local banner.</td>
</tr>
<tr>
<td>`ip auth-proxy auth-proxy-banner http [banner-text</td>
<td>file-path]`</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C</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>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Central Web Authentication

Central Web Authentication (CWA) is a process where a policy server, like Cisco Identity Services Engine (ISE), is used to centrally authenticate users via Web Authentication. Having a central policy server for Web Authentication makes it easier to implement operationally. CWA supports both ACL and VLAN-based enforcement. Additionally, RADIUS CoA is also supported. This allows for posture assessment and enforcement based on profiling.

Note

CWA is introduced for the Catalyst 2960-L switch from Cisco IOS Release 15.2(5)E1.

For details on how to configure Central Web Authentication for all Catalyst switches, refer to the Central Web Authentication with a Switch and Identity Services Engine Configuration Example document.

Removing Web-Based Authentication Cache Entries

Follow these steps to remove web-based authentication cache entries:

**SUMMARY STEPS**

1. enable
2. clear ip admission cache { * | host ip address }

**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 clear ip admission cache { *</td>
<td>host ip address }</td>
</tr>
<tr>
<td>Example: Switch# clear ip admission cache 192.168.4.5</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring Web-Based Authentication Status

Use the commands in this topic to display the web-based authentication settings for all interfaces or for specific ports.

Table 102: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication sessions method webauth</td>
<td>Displays the web-based authentication settings for all interfaces for fastethernet, gigabitethernet, or tengigabitethernet</td>
</tr>
<tr>
<td>show wireless client mac-address a.a.a detail</td>
<td>Displays the session specific wireless information and wireless states.</td>
</tr>
<tr>
<td>show authentication sessions interface type slot/port [details]</td>
<td>Displays the web-based authentication settings for the specified interface for fastethernet, gigabitethernet, or tengigabitethernet. In Session Aware Networking mode, use the show access-session interface command.</td>
</tr>
</tbody>
</table>

Displaying Web-Based Authentication Status

Perform this task to display the web-based authentication settings for all interfaces or for specific ports:

SUMMARY STEPS

1. show authentication sessions {interface type/ slot}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 show authentication sessions {interface type/ slot}</td>
<td>Displays the web-based authentication settings. type = fastethernet, gigabitethernet, or tengigabitethernet (Optional) Use the interface keyword to display the web-based authentication settings for a specific interface</td>
</tr>
<tr>
<td>Example:</td>
<td>This example shows how to view only the global web-based authentication status:</td>
</tr>
<tr>
<td>Example:</td>
<td>This example shows how to view the web-based authentication settings for gigabit interface 3/27:</td>
</tr>
</tbody>
</table>

Monitoring HTTP Authentication Proxy

Perform the following task to troubleshoot your HTTP authentication proxy configuration:
**Verifying HTTPS Authentication Proxy**

To verify your HTTPS authentication proxy configuration, perform the following optional steps:

**SUMMARY STEPS**

1. enable
2. show ip admission { status | cache }

**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**
| show ip admission { status | cache }
| Example:
| Device# show ip admission cache |
| Display the network admission configuration status and cache entries for web authentication sessions. |

### Configuration Examples for Web-Based Authentication

**Example: Configuring the Authentication Rule and Interfaces**

This example shows how to enable web-based authentication on Fast Ethernet port 5/1:
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking

This example shows how to verify the configuration:

Switch# show ip admission
IP admission status:
  Enabled interfaces 0
  Total sessions 0
  Init sessions 0  Max init sessions allowed 100
  Limit reached 0  Hi watermark 0
  TCP half-open connections 0  Hi watermark 0
  TCP new connections 0  Hi watermark 0
  TCP half-open + new 0  Hi watermark 0
  HTTPD1 Contexts 0  Hi watermark 0

Parameter Map: Global
  Custom Pages
    Custom pages not configured
  Banner
    Banner not configured

Example: AAA Configuration

aaa new-model
aaa authentication login default group tacacs group radius
! Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default group tacacs group radius
! Define the AAA servers used by the router.
aaa accounting auth-proxy default start-stop group tacacs+
! Set up authentication proxy with accounting.
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco

Example: HTTP Server Configuration

! Enable the HTTP server on the router.
ip http server
! Set the HTTP server authentication method to AAA.
ip http authentication aaa
! Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61

Example: Customizing the Authentication Proxy Web Pages

This example shows how to configure custom authentication proxy web pages:

Switch(config)# ip admission proxy http login page file flash:login.htm
Example: Specifying a Redirection URL for Successful Login

Configuring redirection URL for successful login

Switch(config)# ip admission proxy http success redirect www.cisco.com

Verifying redirection URL for Successful Login

This example shows how to configure a redirection URL for successful login:

Additional References for Web-Based Authentication

<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>IBNS commands</td>
<td>Cisco IOS Identity-Based Networking Services Command Reference</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 Web-Based Authentication

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature is introduced.</td>
</tr>
</tbody>
</table>
CHAPTER 51

Configuring Port-Based Traffic Control

• Overview of Port-Based Traffic Control, on page 962
• Finding Feature Information, on page 962
• Information About Storm Control, on page 962
• How to Configure Storm Control, on page 964
• Finding Feature Information, on page 966
• Information About Protected Ports, on page 967
• How to Configure Protected Ports, on page 967
• Monitoring Protected Ports, on page 969
• Where to Go Next, on page 969
• Additional References, on page 969
• Feature Information, on page 970
• Finding Feature Information, on page 970
• Information About Port Blocking, on page 970
• How to Configure Port Blocking, on page 971
• Monitoring Port Blocking, on page 972
• Where to Go Next, on page 973
• Additional References, on page 973
• Feature Information, on page 974
• Prerequisites for Port Security, on page 974
• Restrictions for Port Security, on page 974
• Information About Port Security, on page 974
• How to Configure Port Security, on page 978
• Configuration Examples for Port Security, on page 985
• Additional References, on page 986
• Finding Feature Information, on page 987
• Information About Protocol Storm Protection, on page 987
• How to Configure Protocol Storm Protection, on page 988
• Monitoring Protocol Storm Protection, on page 989
• Additional References, on page 989
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

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 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>enable</td>
<td>Enables privileged EXEC mode.</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>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</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>4</td>
<td>`storm-control action {shutdown</td>
<td>trap}`</td>
</tr>
</tbody>
</table>
|      |                  | • Select the `shutdown` keyword to error-disable the port during a storm.  
<p>|      |                  | • Select the <code>trap</code> keyword to generate an SNMP trap when a storm is detected. |
| 5    | <code>storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}</code> | Configures broadcast, multicast, or unicast storm control. By default, storm control is disabled. |
|      |                  | The keywords have these meanings: |
|      |                  | • For <code>level</code>, 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 <code>level-low</code>, 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 <code>bps bps</code>, specifies the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0.</td>
</tr>
<tr>
<td></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></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<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 <strong>0.0 to 10000000000.0</strong>.</td>
</tr>
<tr>
<td>For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**  
Example:  
Switch(config-if)# end  
Returns to privileged EXEC mode.

**Step 7**  
Example:  
Switch# show storm-control gigabitethernet 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**  
Example:  
Switch# copy running-config startup-config  
(Optional) Saves your entries in the configuration file.

### 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 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.

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
### 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>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</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>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></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><strong>Example:</strong></td>
<td></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><code>Switch(config)# interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the interface to be a protected port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>switchport protected</code></td>
<td>Configures the interface to be a protected port.</td>
</tr>
<tr>
<td><code>Switch(config-if)# switchport protected</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</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>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>show interfaces interface-id switchport</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>Switch# show interfaces gigabitethernet 0/1 switchport</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td><code>Switch# show running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring Protected Ports

**Table 103: 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

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the 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 15.2(5)E</td>
<td>This feature was introduced.</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>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Example: Switch&gt; enable</td>
<td>Enables privileged EXEC mode. • 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>interface interface-id</td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport block multicast</td>
<td>Blocks unknown multicast forwarding out of the port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>Note Pure Layer 2 multicast traffic as well as multicast packets that contain IPv6 information in the header are blocked.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# switchport block multicast</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

---

### Monitoring Port Blocking

**Table 104: Commands for Displaying Port Blocking Settings**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces [interface-id] switchport</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>

---

Security


**Where to Go Next**

- Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Message Decoder</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</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></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:


### 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

### Feature Information

<table>
<thead>
<tr>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</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 985

### 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.

#### Note

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 105: 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>

14 Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.

15 The switch returns an error message if you manually configure an address that would cause a security violation.

16 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 984
Default Port Security Configuration

Table 106: 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. Static aging is disabled. 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 107: 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>

17 DTP=Dynamic Trunking Protocol
18 A port configured with the **switchport mode dynamic** interface configuration command.
19 A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.
20 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>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:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><code>Switch&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>2.</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>3.</td>
<td><code>port-security mac-address forbidden mac address</code></td>
<td>Specifies a MAC address that should be forbidden by port-security on all the interfaces.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# port-security mac-address forbidden 2.2.2</code></td>
<td></td>
</tr>
<tr>
<td>4.</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>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch(config)# interface gigabitethernet 0/1</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>
<tr>
<td><strong>Step 5</strong> switchport mode {access</td>
<td>trunk}</td>
<td>Sets the interface switchport mode as access or trunk; an interface in the default mode (dynamic auto) cannot be configured as a secure port.</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# switchport mode access</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> switchport voice vlan vlan-id</td>
<td>Enables voice VLAN on a port.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# switchport voice vlan 22</td>
<td>vlan-id—Specifies the VLAN to be used for voice traffic.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> switchport port-security</td>
<td>Enable port security on the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# switchport port-security</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> switchport port-security [maximum value vlan {vlan-list</td>
<td>{access</td>
<td>voice}}]]</td>
</tr>
<tr>
<td><strong>Example:</strong> Switch(config-if)# switchport port-security maximum 20</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Optional) **vlan**—sets a per-VLAN maximum value

Enter one of these options after you enter the **vlan** keyword:

- **vlan-list**—On a trunk port, you can set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
- **access**—On an access port, specifies the VLAN as an access VLAN.
- **voice**—On an access port, specifies the VLAN as a voice VLAN.

**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.
<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switchport port-security violation {protect</td>
<td>restrict</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# switchport port-security violation restrict</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

- **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 or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

- **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.

**Note**

- 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. You can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands or by using the **clear errdisable interface vlan** privileged EXEC command.

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>switchport port-security [mac-address mac-address [vlan vlan-id</td>
<td>access</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice</td>
<td>MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>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>
<td></td>
</tr>
</tbody>
</table>

(Optional) **vlan**—sets a per-VLAN maximum value. Enter one of these options after you enter the **vlan** keyword:

- **vlan-id**—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.
- **access**—On an access port, specifies the VLAN as an access VLAN.
- **voice**—On an access port, specifies the VLAN as a voice VLAN.

**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 11**

**switchport port-security mac-address sticky**

**Example:**

Switch(config-if)# switchport port-security mac-address sticky

(Optional) Enables sticky learning on the interface.

**Step 12**

**switchport port-security mac-address sticky**

**Example:**

Switch(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice

(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, are converted to sticky secure MAC addresses, and are added to the running configuration.

**Note** 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.

(Optional) **vlan**—sets a per-VLAN maximum value. Enter one of these options after you enter the **vlan** keyword:
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>• <strong>access</strong>—On an access port, specifies the VLAN as an access VLAN.</td>
<td></td>
</tr>
<tr>
<td>• <strong>voice</strong>—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.

<table>
<thead>
<tr>
<th>Step 13</th>
<th>switchport port-security mac-address forbidden mac address</th>
<th>Specifies a MAC address that should be forbidden by port-security on the particular interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config-if)# switchport port-security mac-address forbidden 2.2.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th>show port-security</th>
<th>Verifies your entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch# show port-security</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 16</th>
<th>show running-config</th>
<th>Verifies your entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 17</th>
<th>copy running-config startup-config</th>
<th>(Optional) Saves your entries in the configuration file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch# copy running-config startup-config</td>
<td></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>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: enable</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: configure terminal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>interface interface-id</td>
<td>Specifies the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>switchport port-security aging {static</td>
<td>time time</td>
</tr>
<tr>
<td></td>
<td>Example: switchport port-security aging time 120</td>
<td>The switch does not support port security aging of sticky secure addresses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter static to enable aging for statically configured secure addresses on this port.</td>
</tr>
<tr>
<td></td>
<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></td>
<td>For type, select one of these keywords:</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>• absolute</td>
<td>Sets the aging type as absolute aging. All the secure addresses on this port age out exactly after the time (minutes) specified lapses and are removed from the secure address list.</td>
<td></td>
</tr>
<tr>
<td>• inactivity</td>
<td>Sets the aging type as inactivity aging. The secure addresses on this port age out only if there is no data traffic from the secure source addresses for the specified time period.</td>
<td></td>
</tr>
<tr>
<td>Step 5</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>Step 6</td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td>show port-security [interface interface-id] [address]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# show port-security interface gigabitethernet 0/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>Verifies your entries.</td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td></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>Step 8</td>
<td>(Optional) Saves your entries in the configuration file.</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- Port Security Aging, on page 976

**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
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 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 974
  Enabling and Configuring Port Security

Additional References

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the 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>

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.

Note
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></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: <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: <code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Configures protocol storm protection for ARP, IGMP, or DHCP.</td>
</tr>
<tr>
<td>`psp {arp</td>
<td>dhcp</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(config)# psp dhcp pps 35</td>
<td>For value, 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>
</tbody>
</table>

**Step 4**

**errdisable detect cause psp**

*Example:*

Switch(config)# errdisable detect cause psp

(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.

**Step 5**

**errdisable recovery interval time**

*Example:*

Switch

(Optional) Configures an auto-recovery time (in seconds) for error-disabled virtual ports. When a virtual port is error-disabled, the switch auto-recovers after this time. The range is from 30 to 86400 seconds.

**Step 6**

**end**

*Example:*

Switch(config)# end

Returns to privileged EXEC mode.

**Step 7**

**show psp config {arp | dhcp | igmp}**

*Example:*

Switch# show psp config dhcp

Verifies your entries.

---

**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**

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the 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>
PART IX

System Management

• Administering the System, on page 993
• Performing Switch Setup Configuration, on page 1025
• Configuring System Message Logs, on page 1051
• Configuring Online Diagnostics, on page 1065
• Troubleshooting the Software Configuration, on page 1075
Administering the System

• Information About Administering the Switch, on page 993
• How to Administer the Switch, on page 1000
• Monitoring and Maintaining Administration of the Switch, on page 1020
• Configuration Examples for Switch Administration, on page 1021
• Feature History and Information for Switch Administration, on page 1024

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 below 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 74: 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 75: 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*.

**Default System Name and Prompt Configuration**

The default switch system name and prompt is *Switch*.

**DNS**

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).
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>
<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

For complete syntax and usage information for the commands used in this section, see the command reference for this release.
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.

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`

### 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> Switch&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> Use one of the following:</td>
<td></td>
</tr>
<tr>
<td>- <code>clock set hh:mm:ss day month year</code></td>
<td>Manually set the system clock using one of these formats:</td>
</tr>
<tr>
<td>- <code>clock set hh:mm:ss month day year</code></td>
<td>- <code>hh:mm:ss</code>—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><strong>Example:</strong></td>
<td>- <code>day</code>—Specifies the day by date in the month.</td>
</tr>
</tbody>
</table>
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>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>clock timezone zone hours-offset [minutes-offset]</td>
<td>Sets the time zone.</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# clock timezone AST -3 30</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>
<tr>
<td></td>
<td></td>
<td>• zone—Enters the name of the time zone to be displayed when standard time is in effect. The default is UTC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• hours-offset—Enters the hours offset from UTC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (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.</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>
</tbody>
</table>
### 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

**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> clock summer-time zone date date month year hh:mm date month year hh:mm [offset]</td>
<td>Configures summer time to start and end on specified days every year.</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(config)# clock summer-time PDT date 10 March 2013 2:00 3 November 2013 2:00</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 4** clock summer-time zone recurring \[week day month hh:mm weekday month hh:mm [offset]]\] | 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 `clock summer-time zone recurring` 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.  
  * `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. |
| **Example:** | |
| Switch(config)# clock summer-time PDT recurring 10 March 2013 2:00 3 November 2013 2:00 | |
| **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:** | |
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. |
| **Step 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]] | 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...). |
Configuring a System Name

Follow these steps to manually configure a system name:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. hostname name
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>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch&gt; enable</td>
</tr>
</tbody>
</table>

Enables privileged EXEC mode.

- Enter your password if prompted.

---

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>- (Optional) For hh:mm, specify the time (24-hour format) in hours and minutes.</td>
</tr>
<tr>
<td>- (Optional) For offset, specify the number of minutes to add during summer time. The default is 60.</td>
</tr>
</tbody>
</table>

**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.
### Purpose

**Command or Action** | **Purpose**
---|---
**Step 2** | `configure terminal`<br>**Example:**<br>Switch# configure terminal
| Enters global configuration mode.

**Step 3** | `hostname name`<br>**Example:**<br>Switch(config)# hostname remote-users
| Configures a system name. When you set the system name, it is also used as the system prompt.

| The default setting is Switch.

| The name must follow the rules for ARPANET hostnames.

| They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens.

| Names can be up to 63 characters.

**Step 4** | `end`<br>**Example:**<br>remote-users(config)# end
| Returns to privileged EXEC mode.

**Step 5** | `show running-config`<br>**Example:**<br>Switch# show running-config
| Verifies your entries.

**Step 6** | `copy running-config startup-config`<br>**Example:**<br>Switch# copy running-config startup-config
| (Optional) Saves your entries in the configuration file.

### 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>
</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** ip domain-name name | Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).  
| Example: Switch(config)# ip domain-name Cisco.com | Do not include the initial period that separates an unqualified name from the domain name.  
| | 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). |
| **Step 4** ip name-server server-address1 [server-address2 ... server-address6] | Specifies the address of one or more name servers to use for name and address resolution.  
| Example: Switch(config)# ip name-server 192.168.1.100 192.168.1.200 192.168.1.300 | 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. |
| **Step 5** ip domain-lookup [nsap | source-interface interface] | (Optional) Enables DNS-based hostname-to-address translation on your switch. This feature is enabled by default.  
| Example: Switch(config)# ip domain-lookup | 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). |
### 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 *message* 
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: | Enters global configuration mode. |
### 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:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. banner login \textit{c} \textit{message} \textit{c}
4. end
5. show running-config
6. copy running-config startup-config

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Specifies the message of the day.</td>
</tr>
</tbody>
</table>

**Step 3**

<table>
<thead>
<tr>
<th>banner motd \textit{c} \textit{message} \textit{c}</th>
<th>\textit{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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>\textit{message}—Enters a banner message up to 255 characters. You cannot use the delimiting character in the message.</td>
</tr>
<tr>
<td>Switch(config)# banner motd #</td>
<td>This is a secure site. Only authorized users are allowed. For access, contact technical support.</td>
</tr>
<tr>
<td></td>
<td>#</td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>show running-config</th>
<th>Verifies your entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show running-config</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

<table>
<thead>
<tr>
<th>copy running-config startup-config</th>
<th>(Optional) Saves your entries in the configuration file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# copy running-config startup-config</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:</td>
<td></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>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> banner login <code>c message c</code></td>
<td>Specifies the login message.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>switch(config)# banner login $</code></td>
<td><code>c</code>—Enters the delimiting character of your choice, for example, a pound sign (#), and press the Return key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded.</td>
</tr>
<tr>
<td>Access for authorized users only.</td>
<td><code>message</code>—Enters a login message up to 255 characters. You cannot use the delimiting character in the message.</td>
</tr>
<tr>
<td>Please enter your username and password.</td>
<td></td>
</tr>
<tr>
<td>$</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><code>switch(config)# end</code></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><code>switch# show running-config</code></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><code>switch# copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

### 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 | 10-1000000] [routed-mac | vlan 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>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> mac address-table aging-time [0</td>
<td>10-1000000] [routed-mac</td>
</tr>
<tr>
<td>Example:</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>
<tr>
<td>Switch(config)# mac address-table aging-time 500 vlan 2</td>
<td>vlan-id—Valid IDs are 1 to 4094.</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 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><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> `snmp-server host host-addr community-string notification-type { informs</td>
<td>traps } {version {1</td>
</tr>
<tr>
<td>Example: Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification</td>
<td></td>
</tr>
</tbody>
</table>

- `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.
<table>
<thead>
<tr>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• notification-type</strong>—Uses the <code>mac-notification</code> keyword.</td>
<td></td>
</tr>
<tr>
<td><strong>• vrf vrf instance name</strong>—Specifies the VPN routing/forwarding instance for this host.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**
`snmp-server enable traps mac-notification change`

**Example:**
```
Switch(config)# snmp-server enable traps
 mac-notification change
```

Enables the switch to send MAC address change notification traps to the NMS.

**Step 5**
`mac address-table notification change`

**Example:**
```
Switch(config)# mac address-table
 notification change
```

Enables the MAC address change notification feature.

**Step 6**
`mac address-table notification change [interval value] [history-size value]`

**Example:**
```
Switch(config)# mac address-table
 notification change interval 123
Switch(config)# mac address-table
 notification change history-size 100
```

Enters the trap interval time and the history table size.

- (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.

**Step 7**
`interface interface-id`

**Example:**
```
Switch(config)# interface
gigabitethernet 0/2
```

Enters interface configuration mode, and specifies the Layer 2 interface on which to enable the SNMP MAC address notification trap.

**Step 8**
`snmp trap mac-notification change {added | removed}`

**Example:**
```
Switch(config-if)# snmp trap
 mac-notification change added
```

Enables the MAC address change notification trap on the interface.

- Enables the trap when a MAC address is `added` on this interface.
- Enables the trap when a MAC address is `removed` from this interface.

**Step 9**
`end`

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

Returns to privileged EXEC mode.
### 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`
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><code>Example:</code></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><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the recipient of the trap message.</td>
</tr>
<tr>
<td>`snmp-server host host-addr {traps</td>
<td>informs} {version {1</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification</code></td>
<td>• <strong>traps</strong> (the default)—Sends SNMP traps to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4:</td>
<td>snmp-server enable traps mac-notification move</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# snmp-server enable traps mac-notification move</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5:</td>
<td>mac address-table notification mac-move</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# mac address-table notification mac-move</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6:</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 7:</td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show running-config</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8:</td>
<td><code>copy running-config startup-config</code></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>
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.

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 [limit percentage] | [interval time]`
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><code>enable</code></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><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>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>`snmp-server host host-addr {traps</td>
<td>informs} {version {1</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• <code>host-addr</code>—Specifies the name or address of the NMS.</td>
</tr>
<tr>
<td></td>
<td>Switch(config)# snmp-server host 172.20.10.10 traps private</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>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| `mac-notification` | • `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. You can set this string by using the `snmp-server host` command, but 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. |
| `snmp-server enable traps mac-notification threshold` | Enables MAC threshold notification traps to the NMS. |
| `mac address-table notification threshold` | Enables the MAC address threshold notification feature. |
| `mac address-table notification threshold [limit percentage] [interval time]` | Enters the threshold value for the MAC address threshold usage monitoring.  
• (Optional) `limit percentage`—Specifies the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent.  
• (Optional) `interval time`—Specifies the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds. |
| `end` | Returns to privileged EXEC mode. |
| `show running-config` | Verifies your entries. |
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>
<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>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>mac address-table static mac-addr vlan vlan-id interface interface-id</code></td>
<td>Adds a static address to the MAC address table.</td>
</tr>
<tr>
<td>Example:</td>
<td>• <code>mac-addr</code>—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.</td>
</tr>
<tr>
<td><code>Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet 0/1</code></td>
<td>• <code>vlan-id</code>—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• <code>interface-id</code>—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</td>
</tr>
</tbody>
</table>
### 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`

**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;<strong>Example:</strong>&lt;br&gt;<code>Switch&gt; enable</code>&lt;br&gt;Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Monitoring and Maintaining Administration of the Switch

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Enables unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>mac address-table static mac-addr vlan vlan-id drop</strong></td>
<td>Enables unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop</td>
<td>• <em>mac-addr</em>—Specifies a source or destination unicast MAC address (48-bit). Packets with this MAC address are dropped.</td>
</tr>
<tr>
<td></td>
<td>• <em>vlan-id</em>—Specifies the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.</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 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></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>

### 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 mac-address</td>
<td>Removes a specific MAC address.</td>
</tr>
<tr>
<td>clear mac address-table dynamic interface interface-id</td>
<td>Removes all addresses on the specified physical port or port channel.</td>
</tr>
<tr>
<td>clear mac address-table dynamic vlan vlan-id</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>
</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
```
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.
User Access Verification
Password:

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:

Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet1/1

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.

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
# Feature History and Information for Switch Administration

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Performing Switch Setup Configuration

- Information About Performing Switch Setup Configuration, on page 1025
- How to Perform Switch Setup Configuration, on page 1035
- Configuration Examples for Performing Switch Setup, on page 1048

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 110: 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>
<tr>
<td>Telnet password</td>
<td>No password is defined.</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 76: 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 DHCPDISCOVER 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 DCHP 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 over write 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, ciscoconfig.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 ciscoconfig.cfg file (known as the default configuration files).

• The router-config or the ciscortr.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.

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-confg or cisconet.cfg default configuration file. (If the network-confg 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-confg or hostname.cfg, depending on whether network-confg 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-confg, cisconet.cfg, or the hostname file, it reads the router-confg file. If the switch cannot read the router-confg 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 111: 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 <strong>BOOT filesystem :[/file-url ...</strong></td>
<td><strong>boot system filesystem :[/file-url ...</strong></td>
</tr>
<tr>
<td></td>
<td>A semicolon-separated list of executable files to try to</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>load and execute when automatically booting. If the <strong>BOOT</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>environment variable is not set, the system attempts to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>load and execute the first executable image it can find</td>
<td></td>
</tr>
<tr>
<td></td>
<td>by using a recursive, depth-first search through the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>flash filesystem. If the <strong>BOOT</strong> variable is set but</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the specified images cannot be loaded, the system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>attempts to boot the first bootable file that it can</td>
<td></td>
</tr>
<tr>
<td></td>
<td>find in the flash filesystem.</td>
<td></td>
</tr>
<tr>
<td>MANUAL_BOOT</td>
<td>set <strong>MANUAL_BOOT yes</strong></td>
<td><strong>boot manual</strong></td>
</tr>
<tr>
<td></td>
<td>Decides whether the switch automatically or manually</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>boots. Valid values are 1, yes, 0, and no. If it is set</td>
<td>The next time you reboot the system, the switch is in boot loader mode. To boot up the system, use the <strong>boot flash: filesystem :[/file-url boot</strong></td>
</tr>
<tr>
<td></td>
<td>to no or 0, the boot loader attempts to automatically</td>
<td>loader command, and specify the name of the bootable image.</td>
</tr>
<tr>
<td></td>
<td>boot up the system. If it is set to anything else, you</td>
<td></td>
</tr>
<tr>
<td></td>
<td>must manually boot up the switch from the boot loader</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mode.</td>
<td></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.

### Variables and Commands

<table>
<thead>
<tr>
<th>Variable</th>
<th>Boot Loader Command</th>
<th>Cisco IOS Global Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONFIG_FILE</td>
<td>set CONFIG_FILE</td>
<td>boot config-file flash:file-url</td>
</tr>
<tr>
<td></td>
<td>flash:/file-url</td>
<td>Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. Changes the CONFIG_FILE environment variable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BAUD</td>
<td>set BAUD baud-rate</td>
<td>line console 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>speed speed-value</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configures the baud rate.</td>
</tr>
<tr>
<td>ENABLE_BREAK</td>
<td>set ENABLE_BREAK</td>
<td>boot enable-break switch yes/no</td>
</tr>
<tr>
<td></td>
<td>yes/no</td>
<td>This command can be issued when the flash filesystem is initialized when ENABLE_BREAK is set to yes.</td>
</tr>
</tbody>
</table>

**Note**

You have the following 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.

## 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></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><code>ip dhcp pool poolname</code></td>
<td>Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# ip dhcp pool pool</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>boot filename</code></td>
<td>Specifies the name of the configuration file that is used as a boot image.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Switch(dhcp-config)# boot config-boot.text</td>
<td>Specifies the subnet network number and mask of the DHCP address pool.</td>
</tr>
</tbody>
</table>

**Step 4**

network network-number mask prefix-length

Example:

Switch(dhcp-config)# network 10.10.10.0 255.255.255.0

**Note**  
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 (/).

**Step 5**

default-router address

Example:

Switch(dhcp-config)# default-router 10.10.10.1

**Step 6**

option 150 address

Example:

Switch(dhcp-config)# option 150 10.10.10.1

**Step 7**

exit

Example:

Switch(dhcp-config)# exit

**Step 8**

tftp-server flash:filename.text

Example:

Switch(config)# tftp-server flash:config-boot.text

**Step 9**

interface interface-id

Example:

Switch(config)# interface gigabitethernet 0/4

**Step 10**

no switchport

Example:

Switch(config-if)# no switchport

Puts the interface into Layer 3 mode.
### 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.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>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>ip dhcp pool poolname</td>
<td>Creates a name for the DHCP server address pool and enter DHCP pool configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip dhcp pool pool1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>boot filename</td>
<td>Specifies the name of the file that is used as a boot image.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(dhcp-config)# boot config-boot.text</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>network network-number mask prefix-length</td>
<td>Specifies the subnet network number and mask of the DHCP address pool.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(dhcp-config)# network 10.10.10.0 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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>
<td></td>
</tr>
<tr>
<td>5</td>
<td>default-router address</td>
<td>Specifies the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(dhcp-config)# default-router 10.10.1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>option 150 address</td>
<td>Specifies the IP address of the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(dhcp-config)# option 150 10.10.10.1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>option 125 hex</td>
<td>Specifies the path to the text file that describes the path to the image file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(dhcp-config)# option 125 hex 0000.0009.0a05.08661.7574.6f69.6e73.7461.6c6c.5f64.686370</td>
<td></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>8</td>
<td><code>copy tftp flash filename.txt</code></td>
<td>Uploads the text file to the switch.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# copy tftp flash image.bin</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>copy tftp flash imagename.bin</code></td>
<td>Uploads the tar file for the new image to the switch.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# copy tftp flash image.bin</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>exit</code></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# exit</code></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><code>tftp-server flash: config.text</code></td>
<td>Specifies the Cisco IOS configuration file on the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# tftp-server flash:config-boot.text</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>tftp-server flash: imagename.bin</code></td>
<td>Specifies the image name on the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# tftp-server flash:image.bin</code></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td><code>tftp-server flash: filename.txt</code></td>
<td>Specifies the text file that contains the name of the image file to download</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# tftp-server flash:boot-config.text</code></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>interface interface-id</code></td>
<td>Specifies the address of the client that will receive the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config)# interface gigabitethernet 0/4</code></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><code>no switchport</code></td>
<td>Puts the interface into Layer 3 mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Switch(config-if)# no switchport</code></td>
<td></td>
</tr>
</tbody>
</table>
### 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> <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> <code>boot host dhcp</code></td>
<td>Enables autoconfiguration with a saved configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
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>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** ip default-gateway ip-address | Sets up a default gateway (router).  
  Example:  
  Switch(config)# ip default gateway 10.1.5.1 |
| **Step 4** end | Returns to privileged EXEC mode.  
  Example:  
  Switch(config)# end |
| **Step 5** show ip redirects | Displays the address of the default gateway router to verify the setting.  
  Example:  
  Switch# show ip redirects |
| **Step 6** copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
  Example:  
  Switch# copy running-config startup-config |

### Manually Assigning IP Information to Multiple SVIs

This task describes how to manually assign IP information to multiple switched virtual interfaces (SVIs):

**SUMMARY STEPS**

1. configure terminal
2. interface vlan vlan-id
3. ip address ip-address subnet-mask
4. exit
5. ip default-gateway ip-address
6. end
7. show interfaces vlan *vlan-id*
8. show ip redirects

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>interface vlan <em>vlan-id</em></strong></td>
<td>Enters interface configuration mode, and enter the VLAN to which the IP information is assigned. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface vlan 99</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><strong>ip address <em>ip-address</em> subnet-mask</strong>*</td>
<td>Enters the IP address and subnet mask.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-vlan)# ip address 10.10.10.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><strong>exit</strong></td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-vlan)# exit</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>ip default-gateway <em>ip-address</em></strong></td>
<td>Enters the IP address of the next-hop router interface that is directly connected to the switch where a default gateway is being configured. The default gateway receives IP packets with unresolved destination IP addresses from the switch. Once the default gateway is configured, the switch has connectivity to the remote networks with which a host needs to communicate.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# ip default-gateway 10.10.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>When your switch is configured to route with IP, it does not need to have a default gateway set.</td>
</tr>
<tr>
<td>6</td>
<td><strong>end</strong></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)# end</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 7</strong></td>
<td>Verifies the configured IP address.</td>
<td></td>
</tr>
<tr>
<td>show interfaces vlan vlan-id</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch# show interfaces vlan 99</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Step 8**                        | Verifies the configured default gateway.     |
| show ip redirects                 |                                              |
| Example:                          |                                              |
| Switch# show ip redirects         |                                              |

### 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></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>
</tbody>
</table>

| **Step 2**                        | Configures the NVRAM buffersize in KB. The valid range for size is from 4096 to 1048576. |
| boot buffersize size              |                                              |
| Example:                           |                                              |
| Switch(config)# boot buffersize 524288 |                                              |

| **Step 3**                        | Returns to privileged EXEC mode.             |
| end                               |                                              |
| Example:                           |                                              |
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>&lt;br&gt;configure terminal&lt;br&gt;Example: Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;boot flash:/file-url&lt;br&gt;Example: Switch(config)# boot flash:config.text</td>
<td>Specifies the configuration file to load during the next boot cycle. &lt;br&gt;file-url—The path (directory) and the configuration filename. Filenames and directory names are case-sensitive.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;end&lt;br&gt;Example:</td>
<td>Returns to privileged EXEC mode.</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>
<tr>
<td><strong>Step 3</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>
</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></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
</tr>
</tbody>
</table>

Verifies your entries.

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:

- For **file-url**—Specifies the path (directory) and the name of the bootable image.

Filenames and directory names are case-sensitive.

(Optimal) Saves your entries in the configuration file.

Switch# copy running-config startup-config
### Command or Action

| Step 2 | copy running-config startup-config  
Example: copy running-config startup-config | Purpose: 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. |

## 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
Switch(config-if)# end

Example: Configuring DHCP Auto-Image Update

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 ^C Caution - Saving Configuration File to NVRAM May Cause You to No longer Automatically Download Configuration Files at Reboot^C
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
Config Download via DHCP: enabled (next boot: enabled)
Switch#

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:
    NVRAM/Config file
      Auto upgrade: yes
      Auto upgrade path:
Example: Configuring NVRAM Buffer Size

buffer size: 600000
Timeout for Config Download: 300 seconds
Config Download via DHCP: enabled (next boot: enabled)

Switch#
CHAPTER 54

Configuring System Message Logs

- Restrictions for Configuring System Message Logs, on page 1051
- Information About Configuring System Message Logs, on page 1051
- How to Configure System Message Logs, on page 1054
- Monitoring and Maintaining System Message Logs, on page 1062
- Configuration Examples for System Message Logs, on page 1062
- Additional References for System Message Logs, on page 1063
- Feature History and Information For System Message Logs, on page 1064

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. 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. If a standalone switch, 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.

---

**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 112: System Log Message Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seq no:</code></td>
<td>Stamps log messages with a sequence number only if the <code>service sequence-numbers</code> global configuration command is configured.</td>
</tr>
<tr>
<td><code>timestamp</code></td>
<td>Date and time of the message or event. This information appears only if the <code>service timestamps log [datetime] [log]</code> global configuration command is configured.</td>
</tr>
<tr>
<td>formats:</td>
<td></td>
</tr>
<tr>
<td><code>mm/dd h h:mm:ss</code></td>
<td></td>
</tr>
<tr>
<td><code>hh:mm:ss</code></td>
<td>(short uptime)</td>
</tr>
<tr>
<td><code>d h</code></td>
<td>(long uptime)</td>
</tr>
<tr>
<td><code>facility</code></td>
<td>The facility to which the message refers (for example, SNMP, SYS, and so forth).</td>
</tr>
<tr>
<td><code>severity</code></td>
<td>Single-digit code from 0 to 7 that is the severity of the message.</td>
</tr>
<tr>
<td><code>MNEMONIC</code></td>
<td>Text string that uniquely describes the message.</td>
</tr>
</tbody>
</table>
Default System Message Logging Settings

Table 113: 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></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Example:</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></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. 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>
<tr>
<td>logging buffered [size]</td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config)# logging buffered 8192</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Logs messages to a UNIX syslog server host.</td>
</tr>
<tr>
<td>logging host</td>
<td>Example:</td>
</tr>
<tr>
<td>Switch(config)# logging 125.1.1.100</td>
<td></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.

**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.
### Command or Action

| 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 |

### Purpose
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.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>

### Purpose
Returns to privileged EXEC mode.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>terminal monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Switch# terminal monitor</td>
</tr>
</tbody>
</table>

### Purpose
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]**
### 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> line [console</td>
<td>vty] line-number [ending-line-number]</td>
</tr>
<tr>
<td>Example: Switch(config)# line console</td>
<td>• console — Specifies configurations that occur through the switch console port or the Ethernet management port.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>You can change the setting of all 16 vty lines at once by entering:</td>
</tr>
<tr>
<td></td>
<td>line vty 0 15</td>
</tr>
<tr>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>line vty 2</td>
</tr>
<tr>
<td></td>
<td>When you enter this command, the mode changes to line configuration.</td>
</tr>
<tr>
<td><strong>Step 3</strong> logging synchronous [level [severity-level</td>
<td>all]</td>
</tr>
<tr>
<td>Example: Switch(config)# logging synchronous level 3 limit 1000</td>
<td>• (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.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) level all — Specifies that all messages are printed asynchronously regardless of the severity level.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) limit number-of-buffers — Specifies the number of buffers to be queued for the terminal after which new messages are dropped. The range is 0 to 2147483647. The default is 20.</td>
</tr>
</tbody>
</table>
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>
<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>no logging console</td>
<td>Disables message logging.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# no logging console</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</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>
</tbody>
</table>
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>
<tbody>
<tr>
<td><strong>Step 1</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 2</strong> Use one of these commands:</td>
<td>Enables log time stamps.</td>
</tr>
<tr>
<td>• service timestamps log uptime</td>
<td>• <strong>log uptime</strong>—Enables time stamps on log messages, showing the time</td>
</tr>
<tr>
<td>• service timestamps log datetime</td>
<td>since the system was rebooted.</td>
</tr>
<tr>
<td>[msec</td>
<td>localtime</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# service timestamps</td>
<td></td>
</tr>
<tr>
<td>log uptime</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# service timestamps</td>
<td></td>
</tr>
<tr>
<td>log datetime</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</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>

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.
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
3. logging monitor level
4. logging trap level
5. end

DETAILED STEPS

<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>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>logginglevel</td>
<td></td>
</tr>
<tr>
<td>loggingmonitorlevel</td>
<td></td>
</tr>
<tr>
<td>loggingtrappevel</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>
</tbody>
</table>
### Command or Action

**Step 2**
- `logging console level`
- **Example:**
  
  Switch(config)# logging console 3

**Step 3**
- `logging monitor level`
- **Example:**
  
  Switch(config)# logging monitor 3

**Step 4**
- `logging trap level`
- **Example:**
  
  Switch(config)# logging trap 3

**Step 5**
- `end`
- **Example:**
  
  Switch(config)# end

### Purpose

**Limits messages logged to the console.**

By default, the console receives debugging messages and numerically lower levels.

**Limits messages logged to the terminal lines.**

By default, the terminal receives debugging messages and numerically lower levels.

**Limits messages logged to the syslog servers.**

By default, syslog servers receive informational messages and numerically lower levels.

**Returns to privileged EXEC mode.**

---

### 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>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>
### Purpose

Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChangesthedefaultlevelofsyslogmessagesstoredinthehistoryfileandsenttotheSNMPserver. By default, warnings, errors, critical, alerts, and emergencies messages are sent.</td>
</tr>
<tr>
<td>Specifiesthenumberofsyslogmessagesthatcanbestoredinthehistorytable. The default is to store one message. The range is 0 to 500 messages.</td>
</tr>
<tr>
<td>Returns to privileged EXEC mode.</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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a line to the file /etc/syslog.conf.</td>
<td><strong>local7</strong>—Specifies the logging facility.</td>
</tr>
</tbody>
</table>
### Monitoring and Maintaining System Message Logs

#### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>local7.debug /usr/adm/logs/cisco.log</td>
<td><em>debug</em>—Specifies the syslog level. The file must already exist, and the syslog daemon must have permission to write to it.</td>
</tr>
</tbody>
</table>

#### Step 2

Enter these commands at the UNIX shell prompt.

**Example:**

```shell
$ 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:**

```shell
$ 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
*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)
```
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) (Switch-2)
```

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

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>System message log commands</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.</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 History and Information For System Message Logs

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Chapter 55

Configuring Online Diagnostics

- Information About Configuring Online Diagnostics, on page 1065
- How to Configure Online Diagnostics, on page 1066
- Monitoring and Maintaining Online Diagnostics, on page 1070
- Configuration Examples for Online Diagnostic Tests, on page 1070

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>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Starts the diagnostic tests. You can specify the tests by using one of these options:</td>
</tr>
<tr>
<td>*diagnostic start test {name</td>
<td>test-id</td>
</tr>
<tr>
<td></td>
<td><em>test-id—Enters the ID number of the test.</em></td>
</tr>
<tr>
<td></td>
<td><em>test-id-range—Enters the range of test IDs by using integers separated by a comma and a hyphen.</em></td>
</tr>
<tr>
<td></td>
<td><em>all—Starts all of the tests.</em></td>
</tr>
<tr>
<td></td>
<td><em>basic—Starts the basic test suite.</em></td>
</tr>
<tr>
<td></td>
<td><em>non-disruptive—Starts the non-disruptive test suite.</em></td>
</tr>
</tbody>
</table>

 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}`
## 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`

### 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><em>Example:</em> Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Schedules on-demand diagnostic tests for a specific day and time.</td>
</tr>
<tr>
<td>`diagnostic schedule test {name</td>
<td>test-id</td>
</tr>
<tr>
<td><em>Example:</em> Switch(config)# diagnostic schedule test 1-5 on July 3 2013 23:10</td>
<td></td>
</tr>
</tbody>
</table>

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.
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} all
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** diagnostic monitor interval test `{name | test-id | test-id-range | all} hh:mm:ss milliseconds day | Configures the health-monitoring interval of the specified tests.  
  When specifying the tests, use one of these parameters:  
  - *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 of the diagnostic tests.  
  When specifying the interval, set these parameters:  
  - *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.  
  - *milliseconds*—Monitoring interval in milliseconds (ms). The range is from 0 to 999.  
  - *day*—Monitoring interval in the number of days. The range is from 0 to 20.  
  Example:  
  Switch(config)# diagnostic monitor interval test  
  1 12:30:00 750 5 |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 4    | diagnostic monitor syslog  
**Example:**  
Switch(config)# diagnostic monitor syslog | (Optional) Configures the switch to generate a syslog message when a health-monitoring test fails. |
| 5    | diagnostic monitor threshold number test {name | test-id | test-id-range | all} failure count count  
**Example:**  
Switch(config)# diagnostic monitor threshold test 1 failure count 20 | (Optional) Sets the failure threshold for the health-monitoring tests.  
When specifying the tests, use one of these parameters:  
• *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 of the diagnostic tests.  
The range for the failure threshold `count` is 0 to 99. |
| 6    | diagnostic monitor test {name | test-id | test-id-range | all}  
**Example:**  
Switch(config)# diagnostic monitor test 1 | Enables the specified health-monitoring tests.  
When specifying the tests, use one of these parameters:  
• *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 of the diagnostic tests. |
| 7    | end  
**Example:**  
Switch(config)# end | Returns to privileged EXEC mode. |
| 8    | show running-config  
**Example:**  
Switch# show running-config | Verifies your entries. |
| 9    | copy running-config startup-config  
**Example:** | (Optional) Saves your entries in the configuration file. |
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 114: Commands for Diagnostic Test Configuration and Results**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diagnostic content</code></td>
<td>Displays the online diagnostics configured for a switch.</td>
</tr>
<tr>
<td><code>show diagnostic status</code></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><code>show diagnostic detail</code></td>
<td>Displays the online diagnostics test results.</td>
</tr>
<tr>
<td><code>show diagnostic schedule</code></td>
<td>Displays the online diagnostics test schedule.</td>
</tr>
<tr>
<td><code>show diagnostic post</code></td>
<td>Displays the POST results. (The output is the same as the <code>show post</code> 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>
</table>
|        | diagnostic start test \{name | test-id | test-id-range | all | basic | non-disruptive \} | Starts the diagnostic tests. 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:

```
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

<table>
<thead>
<tr>
<th>Card</th>
<th>Description</th>
<th>Current Running Test</th>
<th>Run by</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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
Diagnostic is not scheduled.
CHAPTER 56

Troubleshooting the Software Configuration

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 1075
- How to Troubleshoot the Software Configuration, on page 1081
- Verifying Troubleshooting of the Software Configuration, on page 1095
- Scenarios for Troubleshooting the Software Configuration, on page 1098
- Configuration Examples for Troubleshooting Software, on page 1100
- Additional References for Troubleshooting Software Configuration, on page 1102
- Feature History and Information for Troubleshooting Software Configuration, on page 1103

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.

**Note**

**Related Topics**

- Recovering from a Lost or Forgotten Password

---

**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-L Switch Interface and Hardware Component Configuration Guide*.

**Related Topics**

- Scenarios to Troubleshoot Power over Ethernet (PoE), on page 1098

---

**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 1092
- [Example: Pinging an IP Host](#), on page 1100

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 1093
- Example: Performing a Traceroute to an IP Host, on page 1101

**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 1093
Example: Enabling All System Diagnostics, on page 1102

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.
• Environment data—Unique device identifier (UDI) information for a standalone Switch 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.
• Power over Ethernet (PoE)—Record of the power consumption of PoE ports on a standalone Switch.
• Temperature—Temperature of a standalone Switch.
• Uptime data—Time when a standalone Switch 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.

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.
Possible Symptoms of High CPU Utilization

Excessive CPU utilization might result in these symptoms, but the symptoms might also result from other causes:

- 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

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.

---

**Recovered 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.

**Note**
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.

**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**  Initialize the 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:
  13 drwx 192 Mar 01 2013 22:30:48
c2960x-universalk9-mz-150-2.EX1/c2960x-universalk9-mz-150-2.EX1.bin
  11 -rwx 5825 Mar 01 2013 22:31:59 config.text

16128000 bytes total (10003456 bytes free)
```
Step 5
Renamed 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.
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.

**Note**

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 file system 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.

**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 standalone 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:**
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

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 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.
Replacing a Failed Command Switch with Another Switch

To replace a failed command switch with a switch that is command-capable but not part of the cluster, follow these steps:

**Step 1**
Insert the new switch in place of the failed command switch, and duplicate its connections to the cluster members.

**Step 2**
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 the switch hardware installation guide.

**Step 3**
At the switch prompt, enter privileged EXEC mode.

*Example:*
```
Switch> enable
Switch#
```

**Step 4**
Enter the password of the **failed command switch**.

**Step 5**
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 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 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.

---

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.

---

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 reinser 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping ip host</td>
<td>Pings a remote host through IP or by supplying the hostname or network address.</td>
</tr>
</tbody>
</table>

Switch# ping 172.20.52.3

Related Topics

Ping, on page 1077

Example: Pinging an IP Host, on page 1100

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).
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>Table 115: Monitoring the Physical Path</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td><code>tracert mac [interface interface-id] {source-mac-address} {interface interface-id} {destination-mac-address} [vlan vlan-id] [detail]</code></td>
</tr>
<tr>
<td>`tracert mac ip {source-ip-address</td>
</tr>
</tbody>
</table>

Executing IP Traceroute

Though other protocol keywords are available with the `traceroute` privileged EXEC command, they are not supported in this release.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `traceroute ip host`
`Switch# traceroute ip 192.51.100.1` | Traces the path that packets take through the network. |

Related Topics

- IP Traceroute, on page 1078
- Example: Performing a Traceroute to an IP Host, on page 1101

Running TDR and Displaying the Results

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.
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.

Related Topics
Debug Commands, on page 1080

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

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.

- 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 1080
Displaying OBFL Information
## Verifying Troubleshooting of the Software Configuration

### Displaying OBFL Information

*Table 116: Commands for Displaying OBFL Information*

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show logging onboard [module[switch-number ]]cliolog</code></td>
<td>Displays the OBFL CLI commands that were entered on a standalone switch.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 cliolog</td>
<td></td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] environment</code></td>
<td>Displays the UDI information for a standalone switch and for all the connected FRU devices: the PID, the VID, and the serial number.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 environment</td>
<td></td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] message</code></td>
<td>Displays the hardware-related messages generated by a standalone switch.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 message</td>
<td></td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] poe</code></td>
<td>Displays the power consumption of PoE ports on a standalone switch.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 poe</td>
<td></td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] temperature</code></td>
<td>Displays the temperature of a standalone switch or.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 temperature</td>
<td></td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] uptime</code></td>
<td>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 have been running since they last restarted.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 uptime</td>
<td></td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] voltage</code></td>
<td>Displays the system voltages of a standalone switch.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 voltage</td>
<td></td>
</tr>
<tr>
<td><code>show logging onboard [module[switch-number ]] continuous</code></td>
<td>Displays the data in the continuous file.</td>
</tr>
<tr>
<td>Switch# show logging onboard 1 continuous</td>
<td></td>
</tr>
</tbody>
</table>
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 117: 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>
<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 118: 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 <code>power inline never</code> is not configured on that interface or port. 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. <strong>Note</strong> Cisco powered device works only with straight cable and not with crossover one. 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>
</tbody>
</table>
### Symptom or Problem

<table>
<thead>
<tr>
<th>Symptom or Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>No PoE on all ports or a group of ports.</td>
</tr>
<tr>
<td>Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an</td>
</tr>
<tr>
<td>Ethernet link on any port, and PoE devices do not power on.</td>
</tr>
</tbody>
</table>

### Possible Cause and Solution

<table>
<thead>
<tr>
<th>Possible Cause and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>If there is a continuous, intermittent, or reoccurring alarm related to power, replace</td>
</tr>
<tr>
<td>the power supply if possible it is a field-replaceable unit. Otherwise, replace the</td>
</tr>
<tr>
<td>switch.</td>
</tr>
<tr>
<td>If the problem is on a consecutive group of ports but not all ports, the power supply</td>
</tr>
<tr>
<td>is probably not defective, and the problem could be related to PoE regulators in the</td>
</tr>
<tr>
<td>switch.</td>
</tr>
<tr>
<td>Use the <code>show log</code> privileged EXEC command to review alarms or system messages that</td>
</tr>
<tr>
<td>previously reported PoE conditions or status changes.</td>
</tr>
<tr>
<td>If there are no alarms, use the <code>show interface status</code> command to verify that the</td>
</tr>
<tr>
<td>ports are not shut down or error-disabled. If ports are error-disabled, use the <code>shut</code></td>
</tr>
<tr>
<td>and <code>no shut</code> interface configuration commands to reenable the ports.</td>
</tr>
<tr>
<td>Use the <code>show env power</code> and <code>show power inline</code> privileged EXEC commands to review the</td>
</tr>
<tr>
<td>PoE status and power budget (available PoE).</td>
</tr>
<tr>
<td>Review the running configuration to verify that <code>power inline never</code> is not configured</td>
</tr>
<tr>
<td>on the ports.</td>
</tr>
<tr>
<td>Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch</td>
</tr>
<tr>
<td>cord. Do not use the existing distribution cables. Enter the <code>shut</code> and <code>no shut</code></td>
</tr>
<tr>
<td>interface configuration commands, and verify that an Ethernet link is established. If</td>
</tr>
<tr>
<td>this connection is good, use a short patch cord to connect a powered device to this</td>
</tr>
<tr>
<td>port and verify that it powers on. If the device powers on, verify that all intermediate</td>
</tr>
<tr>
<td>patch panels are correctly connected.</td>
</tr>
<tr>
<td>Disconnect all but one of the Ethernet cables from switch ports. Using a short patch</td>
</tr>
<tr>
<td>cord, connect a powered device to only one PoE port. Verify the powered device does not</td>
</tr>
<tr>
<td>require more power than can be delivered by the switch port.</td>
</tr>
<tr>
<td>Use the <code>show power inline</code> privileged EXEC command to verify that the powered device</td>
</tr>
<tr>
<td>can receive power when the port is not shut down. Alternatively, watch the powered</td>
</tr>
<tr>
<td>device to verify that it powers on.</td>
</tr>
<tr>
<td>If a powered device can power on when only one powered device is connected to the</td>
</tr>
<tr>
<td>switch, enter the <code>shut</code> and <code>no shut</code> interface configuration commands on the</td>
</tr>
<tr>
<td>remaining ports, and then reconnect the Ethernet cables one at a time to the switch</td>
</tr>
<tr>
<td>PoE ports. Use the <code>show interface status</code> and <code>show power inline</code> privileged EXEC</td>
</tr>
<tr>
<td>commands to monitor inline power statistics and port status.</td>
</tr>
<tr>
<td>If there is still no PoE at any port, a fuse might be open in the PoE section of the</td>
</tr>
<tr>
<td>power supply. This normally produces an alarm. Check the log again for alarms reported</td>
</tr>
<tr>
<td>earlier by system messages.</td>
</tr>
<tr>
<td>Symptom or Problem</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Cisco pre-standard powered device disconnects or resets. After working normally, a Cisco phone intermittently reloads or disconnects from PoE.</td>
</tr>
<tr>
<td>IEEE 802.3af-compliant or IEEE 802.3at-compliant powered devices do 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>
</tr>
</tbody>
</table>

**Related Topics**

- [Power over Ethernet Ports](#), on page 1076

## 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 = 1/24 ms
Switch#

Table 119: 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 (\texttt{Ctrl-^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**
- \texttt{Ping}, on page 1077
- \texttt{Executing Ping}, on page 1092

**Example: Performing a Traceroute to an IP Host**

This example shows how to perform a \texttt{traceroute} to an IP host:

Switch# \texttt{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 120: 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 (Ctrl-^ X by default). Simultaneously press and release the Ctrl, Shift, and 6 keys and then press the X key.

**Related Topics**
- IP Traceroute, on page 1078
- Executing IP Traceroute, on page 1093

## Example: Enabling All System Diagnostics

⚠️ **Caution**

Because debugging output takes priority over other network traffic, and because the `debug all` privileged EXEC command generates more output than any other `debug` command, it can severely diminish switch performance or even render it unusable. In virtually all cases, it is best to use more specific `debug` commands.

This command disables all-system diagnostics:

```
Switch# debug all
```

The `no debug all` privileged EXEC command disables all diagnostic output. Using the `no debug all` command is a convenient way to ensure that you have not accidentally left any `debug` commands enabled.

**Related Topics**
- Debug Commands, on page 1080

## 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

- **Description**
  - 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.

- **Link**
  - [http://www.cisco.com/support](http://www.cisco.com/support)

### 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 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
PART X

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 1107
Working with the Cisco IOS File System, Configuration Files, and Software Images

• Working with the Flash File System, on page 1107
• Working with Configuration Files, on page 1114
• Replacing and Rolling Back Configurations, on page 1126
• Working with Software Images, on page 1130
• Copying Image Files Using TFTP, on page 1132
• Copying Image Files Using FTP, on page 1136
• Copying Image Files Using RCP, on page 1140

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:
### Displaying Available File Systems

#### Table 121: 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><strong>disk</strong> — The file system is for a flash memory device, USB flash, and crashinfo file.</td>
</tr>
<tr>
<td></td>
<td><strong>network</strong> — The file system for network devices; for example, an FTP server or and HTTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>nvram</strong> — The file system is for a NVRAM device.</td>
</tr>
<tr>
<td></td>
<td><strong>opaque</strong> — The file system is a locally generated pseudo file system (for example, the system) or a download interface, such as brimux.</td>
</tr>
<tr>
<td></td>
<td><strong>unknown</strong> — The file system is an unknown type.</td>
</tr>
<tr>
<td>Flags</td>
<td>Permission for file system.</td>
</tr>
<tr>
<td></td>
<td><strong>ro</strong> — read-only.</td>
</tr>
<tr>
<td></td>
<td><strong>rw</strong> — read/write.</td>
</tr>
<tr>
<td></td>
<td><strong>wo</strong> — write-only.</td>
</tr>
</tbody>
</table>
### Prefixes

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes</td>
<td>Alias for file system.</td>
</tr>
<tr>
<td>crashinfo</td>
<td>— Crashinfo file.</td>
</tr>
<tr>
<td>flash</td>
<td>— Flash file system.</td>
</tr>
<tr>
<td>ftp</td>
<td>— FTP server.</td>
</tr>
<tr>
<td>http</td>
<td>— HTTP server.</td>
</tr>
<tr>
<td>https</td>
<td>— Secure HTTP server.</td>
</tr>
<tr>
<td>nvram</td>
<td>— NVRAM.</td>
</tr>
<tr>
<td>null</td>
<td>— Null destination for copies. You can copy a remote file to null to find its size.</td>
</tr>
<tr>
<td>rcp</td>
<td>— Remote Copy Protocol (RCP) server.</td>
</tr>
<tr>
<td>scp</td>
<td>— Session Control Protocol (SCP) server.</td>
</tr>
<tr>
<td>system</td>
<td>— Contains the system memory, including the running configuration.</td>
</tr>
<tr>
<td>tftp</td>
<td>— TFTP network server.</td>
</tr>
<tr>
<td>usbflash0</td>
<td>— USB flash memory.</td>
</tr>
<tr>
<td>xmodem</td>
<td>— Obtain the file from a network machine by using the Xmodem protocol.</td>
</tr>
<tr>
<td>ymodem</td>
<td>— Obtain the file from a network machine by using the Ymodem protocol.</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</th>
<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 | `dir filesystem:`  
Example: Switch# `dir flash:` | Displays the directories on the specified file system.  
For `filesystem:`., use flash: for the system board flash device. |
| Step 3 | `cd directory_name`  
Example: Switch# `cd new_configs` | Navigates to the specified directory.  
The command example shows how to navigate to the directory named `new_configs`. |
| Step 4 | `pwd`  
Example: | Displays the working directory. |

---

### Table 122: Commands for Displaying Information About Files

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dir [/all] [filesystem:filename]</code></td>
<td>Displays a list of files on a file system.</td>
</tr>
<tr>
<td><code>show file systems</code></td>
<td>Displays more information about each of the files on a file system.</td>
</tr>
<tr>
<td><code>show file information file-url</code></td>
<td>Displays information about a specific file.</td>
</tr>
<tr>
<td><code>show file descriptors</code></td>
<td>Displays a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.</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>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><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>Example:</td>
<td><code>dir flash:</code></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><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>Example:</td>
<td><code>mkdir new_configs</code></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><code>dir filesystem:</code></td>
<td>Verifies your entry.</td>
</tr>
<tr>
<td>Example:</td>
<td><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.
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 file systems (`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.

<table>
<thead>
<tr>
<th>Caution</th>
<th>When files are deleted, their contents cannot be recovered.</th>
</tr>
</thead>
</table>

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></td>
<td>Creates a file and adds files to it.</td>
</tr>
<tr>
<td><code>archive tar /create destination-url flash:/file-url</code></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><strong>Example:</strong></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>
<tr>
<td><code>switch# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs</code></td>
<td><strong>flash:</strong></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>• TFTPSyntax:</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays the contents of a file.</td>
</tr>
<tr>
<td><code>archive tar /table source-url</code></td>
<td>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:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Local flash file system syntax:</td>
</tr>
<tr>
<td><code>switch# archive tar /table flash: /new_configs</code></td>
<td><strong>flash:</strong></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**  
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| • FTP syntax:     | FTP syntax:  
| `ftp://[username[password]@location]/directory/-filename` |          |
| • RCP syntax:     | RCP syntax:  
| `rcp://[username@location]/directory/-filename` |          |
| • TFTP syntax:    | 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...]**

**Example:**

```
switch# archive tar /xtract
tftp://172.20.10.30/saved.
flash:/new-configs
```

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**

**Example:**

```
switch# more
flash:/new-configs
```

Displays the contents of any readable file, including a file on a remote file system.

---

### 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. Copy an existing configuration from a switch to a server.
2. Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.
3. Extract the portion of the configuration file with the desired commands, and save it in a new file.
4. 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).
5. Make sure the permissions on the file are set to world-read.

**DETAILED STEPS**

**Step 1** Copy an existing configuration from a switch to a server.
**Step 2** Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC.
**Step 3** Extract the portion of the configuration file with the desired commands, and save it in a new file.
**Step 4** 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).
**Step 5** Make sure the permissions on the file are set to world-read.

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 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 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-read.
- 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. Copy the configuration file to the appropriate TFTP directory on the workstation.
2. Verify that the TFTP server is properly configured.
3. Log into the switch through the console port, the Ethernet management port, or a Telnet session.
4. Download the configuration file from the TFTP server to configure the switch.

**DETAILED STEPS**

**Step 1** Copy the configuration file to the appropriate TFTP directory on the workstation.
**Step 2** Verify that the TFTP server is properly configured.
**Step 3** Log into the switch through the console port, the Ethernet management port, or a Telnet session.
**Step 4** 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:

```
copy tftp://[//location]/directory/[filename] system:running-config
```
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**

**Step 1**
Verify that the TFTP server is properly configured.

**Step 2**
Log into the switch through the console port, the Ethernet management port, or a Telnet session

**Step 3**
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:

- `copy system:running-config tftp://[[//location]/directory]/filename`
- `copy nvram:startup-config tftp://[[//location]/directory]/filename`
- `copy flash[n]:/directory/startup-config tftp://[[//location]/directory]/filename`

The file is uploaded to the TFTP server.

**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-conf
Write file tokyo-conf on host 172.16.2.155? [confirm] y
```

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.
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 username`
3. `ip ftp password 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>
<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 or password (see Steps 2, 3, and 4).</td>
</tr>
<tr>
<td><strong>Step 2</strong> ip ftp username username</td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip ftp password password</td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Do one of the following:</td>
<td>Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.</td>
</tr>
<tr>
<td>- <code>copy system:running-config ftp: [[///[username \[password \[@\]location\[directory \]filename \]</code></td>
<td></td>
</tr>
<tr>
<td>- <code>copy nvram:startup-config ftp: [[///[username \[password \[@\]location\[directory \]filename \]</code></td>
<td></td>
</tr>
</tbody>
</table>

**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:

```bash
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
```
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.

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
```

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:

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>ip ftp username username</code></td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>ip ftp password password</code></td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
**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.

### Preparing 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 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. This step is required only if you override the default remote username (see Steps 2 and 3).</td>
</tr>
<tr>
<td>2</td>
<td>ip rcmd remote-username username</td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>Do one of the following:</td>
<td>Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.</td>
</tr>
</tbody>
</table>
   - copy rcp://[username@location]/directory/filename/system:running-config
   - copy rcp://[username@location]/directory/filename/nvram:startup-config

**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: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rrt2-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]
%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></td>
<td>configure terminal 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></td>
<td><code>ip rcmd remote-username username</code> (Optional) Specify the remote username.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Do one of the following: Using RCP, copy the configuration file from a switch running configuration or startup configuration file to a network server.</td>
</tr>
</tbody>
</table>

Example

This example shows how to copy the running configuration file named switch2-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-confg
Write file switch-confg 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:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host[?] 172.16.101.101
Name of configuration file to write [switch2-confg]?
```
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></td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>archive</code> Enter archive configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>path url</code> Specify the location and filename prefix for the files in the configuration archive</td>
</tr>
</tbody>
</table>
### 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. Make necessary changes to the running configuration.
4. `exit`
5. `configure replace target-url [list] [force] [time seconds] [nolock]`
6. `configure confirm`
7. `copy running-config startup-config`

**DETAILED STEPS**

#### 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**  
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.

`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.

`force`—Replace the running configuration file with the specified saved configuration file without prompting you for confirmation.

`time seconds`—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).

**Note**  
You must first enable the configuration archive before you can use the `time seconds` command line option.

`nolock`—Disable the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replacement operation.

**Step 6**  
`configure confirm`  
(Optional) Confirm replacement of the running configuration with a saved configuration file.

**Note**  
Use this command only if the `time seconds` keyword and argument of the `configure replace` command are specified.

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

---

**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.
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.

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.

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:

```plaintext
system_type:0x00000000:image-name
image_family:xxxx
```
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
image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family:xxxx
board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002
0x40110000
info_end

Table 123: 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.
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 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 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. Copy the image to the appropriate TFTP directory on the workstation. Make sure that the TFTP server is properly configured.
2. Log into the switch through the console port or a Telnet session.
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

Step 1  
Copy the image to the appropriate TFTP directory on the workstation. Make sure that the TFTP server is properly configured.

Step 2  
Log into the switch through the console port or a Telnet session.

Step 3  
`archive download-sw/overwrite/reload tftp: [ //location ] /directory /image-name.tar`

Download the image file from the TFTP 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 `/location`, specify the IP address of the TFTP server.
- For `/directory/image-name.tar` specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Step 4  
`archive download-sw/leave-old-sw/reload tftp: [ //location ] /directory /image-name.tar`

Download the image file from the TFTP 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 `/location`, specify the IP address of the TFTP 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 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.

Note For the download and upload algorithms to operate properly, do not rename image names

---

**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. Make sure the TFTP server is properly configured
2. Log into the switch through the console port or a Telnet session.
3. archive upload-sw tftp://location/directory/image-name.tar

**DETAILED STEPS**

**Step 1**

Make sure the TFTP server is properly configured

---

**Step 2**

Log into the switch through the console port or a Telnet session.

---

**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.

- 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 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.
For the download and upload algorithms to operate properly, do not rename image names.

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.

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 images 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. Verify that the FTP server is properly configured.
2. Log into the switch through the console port or a Telnet session.
3. `configure terminal`
4. `ip ftp username` `username`
5. `ip ftp password` `password`
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`

**DETAILED STEPS**

**Step 1** Verifying the FTP server is properly configured.
Step 2 Log into the switch through the console port or a Telnet session.

Step 3 configure terminal
Enter global configuration mode.
This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).

Step 4 ip ftp username username
(Optional) Change the default remote username.

Step 5 ip ftp password password
(Optional) Change the default password.

Step 6 end
Return to privileged EXEC mode.

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.

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 [ :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.

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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This step is required only if you override</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the default remote username or password (see</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Steps 2, 3, and 4.)</td>
</tr>
<tr>
<td>2</td>
<td><code>ip ftp username username</code></td>
<td>Optional) Change the default remote username</td>
</tr>
<tr>
<td>3</td>
<td><code>ip ftp password password</code></td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>`archive upload-sw ftp: [/ [username [:password[@]</td>
<td>Upload the currently running switch image</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>username:password</code>, specify the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>username and password. These must be</td>
</tr>
<tr>
<td></td>
<td></td>
<td>associated with an account on the FTP server.</td>
</tr>
</tbody>
</table>

---

*Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)*
Purpose

- 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.

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:

```plaintext
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:

```plaintext
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. Verify that the RCP server is properly configured.
2. Log into the switch through the console port or a Telnet session.
3. configure terminal
4. ip rcmd remote-username username
5. end
6. archive download-sw /overwrite/reload
   rcp: [[/username@] /location] /directory /image-name.tar
7. archive download-sw /leave-old-sw/reload
   rcp: [[/ [username@] location] /directory] /image-name.tar

DETAILED STEPS

Step 1
Verify that the RCP server is properly configured.

Step 2
Log into the switch through the console port or a Telnet session.

Step 3
configure terminal
Enter global configuration mode.
This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).

Step 4
ip rcmd remote-username username
(Optional) Specify the remote username.

Step 5
end
Return to privileged EXEC mode.

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 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 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>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>This step is required only if you override the default remote username or password (see Steps 2 and 3.)</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>ip rcmd remote-username username</code></td>
<td>Optional) Specify the remote username.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>end</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>archive upload-sw</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>rcp: [[[// [username@] location] /directory] /image-name.tar</td>
<td></td>
<td>Upload the currently running switch image to the RCP server.</td>
</tr>
</tbody>
</table>

- 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 name of the software image to be uploaded. Directory and image names are case sensitive.
- The image-name.tar is the name of 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.
PART XI

VLAN

• Configuring VTP, on page 1147
• VLANs, on page 1171
• Configuring VLAN Trunks, on page 1187
• Configuring Voice VLANs, on page 1207
Configuring VTP

- Finding Feature Information, on page 1147
- Prerequisites for VTP, on page 1147
- Restrictions for VTP, on page 1148
- Information About VTP, on page 1148
- How to Configure VTP, on page 1156
- Monitoring VTP, on page 1166
- Configuration Examples for VTP, on page 1167
- Where to Go Next, on page 1168
- Additional References, on page 1169
- Feature History and Information for VTP, on page 1169

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**

*Note*

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 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 1164
- Prerequisites for VTP

**VTP Modes**

*Table 124: 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

<table>
<thead>
<tr>
<th>VTP Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP client</td>
<td>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.</td>
</tr>
<tr>
<td>VTP transparent</td>
<td>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 <code>copy running-config startup-config</code> privileged EXEC command.</td>
</tr>
<tr>
<td>VTP off</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### Related Topics
- Prerequisites for VTP
- Configuring VTP Mode, on page 1156
- Example: Configuring Switch as VTP Server, on page 1168

### 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 1160

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 1160

## 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 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.

Related Topics

Configuring VTP on a Per-Port Basis, on page 1163
Configuring a VTP Version 3 Primary Server, on page 1159

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 1158
- Example: Configuring a Switch as the Primary Server, on page 1167

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 1160

Default VTP Configuration

The following table shows the default VTP configuration.

Table 125: 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> 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>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 3** vtp domain *domain-name*  
Example:  
Switch(config)# vtp domain eng_group | 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. |
| **Step 4** vtp mode {client | server | transparent | off} {vlan | mst | unknown}  
Example:  
Switch(config)# vtp mode server | 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. |
| **Step 5** vtp password *password*  
Example:  
Switch(config)# vtp password mypassword | (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. |
| **Step 6** end  
Example:  
Switch(config)# end | Returns to privileged EXEC mode. |
| **Step 7** show vtp status  
Example:  
Switch# show vtp status | Verifies your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display. |
| **Step 8** copy running-config startup-config  
Example:  
Switch# 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. |

**Related Topics**  
[VTP Modes](#), on page 1149
### 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 version 3`
4. `vtp password password [hidden | secret]`
5. `end`
6. `show vtp password`
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></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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> vtp version 3</td>
<td>Enables VTP version 3 on the device. The default is VTP version 1.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# vtp version 3</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> vtp password password [hidden</td>
<td>secret]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# vtp password mypassword hidden</code></td>
<td>• (Optional) <strong>hidden</strong>—Saves the secret key generated from the password string in the nvram:vlans.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>secret</strong>—Directly configures the password. The secret password must contain 32 hexadecimal characters.</td>
</tr>
</tbody>
</table>
### 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 version 3`
2. `vtp primary [vlan | mst] [force]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  - `vtp version 3`  
    
  **Example:**
  
  `Switch(config)# vtp version 3`  
  | Enables VTP version 3 on the device. The default is VTP version 1. |
| **Step 2**
  - `vtp primary [vlan | mst] [force]`  
    
  **Example:**
  
  `Switch# vtp primary vlan force`  
  | 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 **hidden**, you are prompted to reenter the password.
  
  * (Optional) **vlan**—Selects the VLAN database as the takeover feature. This is the default. |

---

**Related Topics**

- [Passwords for the VTP Domain](#), on page 1154
- [Example: Configuring a Switch as the Primary Server](#), on page 1167
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.

- 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.

Caution: 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>
</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** vtp version \{1 \| 2 \| 3\} | Enables the VTP version on the switch. The default is VTP version 1.  
Example:  
Switch(config)# vtp version 2 |
| **Step 4** end | Returns to privileged EXEC mode.  
Example:  
Switch(config)# end |
| **Step 5** show vtp status | Verifies that the configured VTP version is enabled.  
Example:  
Switch# show vtp status |
| **Step 6** copy running-config startup-config | (Optional) Saves your entries in the configuration file.  
Example:  
Switch# copy running-config startup-config |

**Related Topics**
- [VTP Version](#), on page 1154
- [VTP Version 2](#), on page 1151
- [VTP Version 3](#), on page 1151
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`
4. `end`
5. `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><strong>enable</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enables privileged EXEC mode.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Enter your password if prompted.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Switch&gt; enable</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Switch# configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>vtp pruning</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enables pruning in the VTP administrative domain.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>By default, pruning is disabled. You need to enable pruning on only</strong></td>
</tr>
<tr>
<td></td>
<td><strong>one switch in VTP server mode.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Switch(config)# vtp pruning</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Returns to privileged EXEC mode.</strong></td>
</tr>
</tbody>
</table>
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: 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>Identifies an interface, and enters 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>Switch(config)# interface gigabitethernet0/1</td>
<td>Enables VTP on the specified port.</td>
</tr>
</tbody>
</table>

**Step 4**

```text
vtp
```
Example:
```text
Switch(config-if)# vtp
```

**Step 5**

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

**Step 6**

```text
show running-config interface interface-id
```
Example:
```text
Switch# show running-config interface gigabitethernet 0/1
```

**Step 7**

```text
show vtp status
```
Example:
```text
Switch# show vtp status
```

**Related Topics**

[VTP Settings](#), on page 1153

### 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> 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>show vtp status</td>
<td>Checks the VTP configuration revision number.</td>
</tr>
<tr>
<td>Example: Switch# show vtp status</td>
<td>If the number is 0, add the switch to the VTP domain.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td>If the number is greater than 0, follow these substeps:</td>
</tr>
<tr>
<td>vtp domain domain-name</td>
<td>• Write down the domain name.</td>
</tr>
<tr>
<td>Example: Switch(config)# vtp domain domain123</td>
<td>• Write down the configuration revision number.</td>
</tr>
<tr>
<td></td>
<td>• Continue with the next steps to reset the switch configuration revision number.</td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>show vtp status</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>vtp domain domain-name</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td><code>show vtp status</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- [VTP Domain](#), on page 1148
- Prerequisites for VTP
- Domain Names for Configuring VTP, on page 1153

## 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 126: VTP Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vtp counters</td>
<td>Displays counters about VTP messages that have been sent and received.</td>
</tr>
<tr>
<td>show vtp devices [conflict]</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>show vtp interface [interface-id]</td>
<td>Displays VTP status and configuration for all interfaces or the specified interface.</td>
</tr>
<tr>
<td>show vtp password</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>show vtp status</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]
```

Jun 17 01:08:50.758 PST: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 006c.bc4e.2500 has become the primary server for the VLAN VTP feature

Related Topics

- Configuring a VTP Version 3 Password, on page 1158
- Passwords for the VTP Domain, on page 1154
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`:

```bash
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 1156
- VTP Modes, on page 1149

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.

```bash
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.

```bash
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

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 the 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 VTP

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
VLANs

- Finding Feature Information, on page 1171
- Prerequisites for VLANs, on page 1171
- Restrictions for VLANs, on page 1171
- Information About VLANs, on page 1172
- How to Configure VLANs, on page 1176
- Monitoring VLANs, on page 1183
- Configuration Examples, on page 1184
- Where to Go Next, on page 1185

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 256 VLANs in VTP client, server, and transparent modes.

Restrictions for VLANs

The following are restrictions for configuring VLANs:
To avoid warning messages of high CPU utilization with a normal-range VLAN configuration, we recommend that you have no more than 256 VLANs. If a large number of access interfaces or trunk interfaces 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 127: 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)</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>
<tr>
<td>Dynamic access</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>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.</td>
<td>VTP is not required; it has no effect on a voice VLAN.</td>
</tr>
</tbody>
</table>

### 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.

---

Ensure that you delete the vlan.dat file along with the configuration files before you reset the switch configuration using **write erase** command. This ensures that the switch reboots correctly on a reset.

---

### Normal-Range VLAN Configuration Guidelines

Normal-range VLANs are VLANs with IDs from 1 to 1005.

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.)

- 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.

- 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 1178
Assigning Static-Access Ports to a VLAN
Monitoring VLANs
Example: Creating a VLAN Name, on page 1184

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.

Related Topics
Creating an Extended-Range VLAN
Creating an Extended-Range VLAN with an Internal VLAN ID
Monitoring VLANs
Creating an Extended-Range VLAN
Example: Creating an Extended-Range VLAN, on page 1185

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.

### Note

Table 128: Ethernet VLAN Defaults and Range

<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>Extended-range VLANs (VLAN IDs 1006 to 4094) are only saved in the VLAN database in VTP version 3.</td>
<td></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>
<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>

### 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.

### 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)
• 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
• VLAN number to use when translating from one VLAN type to another

You can cause inconsistency in the VLAN database if you attempt to manually delete the vlan.dat file. If you want to modify the VLAN configuration, follow the procedures in this section.

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.

With VTP version 1 and 2, if the switch is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

SUMMARY STEPS

1. enable
2. configure terminal
3. vlan vlan-id
4. name vlan-name
5. end
6. show vlan [name vlan-name | id vlan-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><strong>Example:</strong> Switch&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 2** | configure terminal
Example:
Switch# configure terminal
Enters global configuration mode.

**Step 3** | vlan vlan-id
Example:
Switch(config)# vlan 20
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.
**Note** The available VLAN ID range for this command is 1 to 4094.

**Step 4** | name vlan-name
Example:
Switch(config-vlan)# name test20
(Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the `vlan-id` value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.

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

**Step 6** | show vlan {name vlan-name | id vlan-id}
Example:
Switch# show vlan name test20 id 20
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.

### 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`
4. `end`
5. `show vlan brief`
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>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>no vlan vlan-id</code></td>
<td>Removes the VLAN by entering the VLAN ID.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch(config)# no vlan 4</code></td>
<td></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>
<tr>
<td><strong>Step 5</strong> <code>show vlan brief</code></td>
<td>Verifies the VLAN removal.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Switch# show vlan brief</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>copy running-config startup-config</code></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>
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>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></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Enters the interface to be added to the VLAN.</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>
<tr>
<td>Step 3</td>
<td>switchport mode access</td>
<td>Defines the VLAN membership mode for the port (Layer 2 access port).</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# switchport mode access</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport access vlan vlan-id</td>
<td>Assigns the port to a VLAN. Valid VLAN IDs are 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# switchport access vlan 2</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. 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.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></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)# end</code></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><code>show running-config interface interface-id</code></td>
<td>Verifies the VLAN membership mode of the interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show running-config interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show interfaces interface-id switchport</code></td>
<td>Verifies your entries in the <code>Administrative Mode</code> and the <code>Access Mode VLAN</code> fields of the display.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Switch# show interfaces gigabitethernet 0/1 switchport</code></td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- **Example: Configuring a Port as Access Port**, on page 1184
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `vtp mode transparent`
4. `vlan vlan-id`
5. `mtu mtu size`
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> <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>vtp mode transparent</code></td>
<td>Configures the switch for VTP transparent mode, disabling VTP.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>vtp mode transparent</code></td>
<td><strong>Note</strong> This step is not required for VTP version 3.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>vlan vlan-id</code></td>
<td>Enters an extended-range VLAN ID and enters VLAN configuration mode. The range is 1006 to 4094.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>vlan 2000</code> Switch(config-vlan)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>mtu mtu size</code></td>
<td>Modifies the VLAN by changing the MTU size.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# <code>end</code></td>
<td></td>
</tr>
</tbody>
</table>
### Monitoring VLANs

#### Table 129: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 7**  
  show vlan id *vlan-id*  
  Example:  
  `Switch# show vlan id 2000` | Verifies that the VLAN has been created. |
| **Step 8**  
  copy running-config startup-config  
  Example:  
  `Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

---

**Table 129: Privileged EXEC show Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [vlan vlan-id]</code></td>
<td>Displays characteristics for all interfaces or for the specified VLAN configured on the switch.</td>
</tr>
</tbody>
</table>
| `show vlan [brief | group [group-name name] | id vlan-id | ifindex | internal | mtu | name name summary ] ]` | 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.  
  - **summary**—Displays a summary of VLAN information. |
### 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:

```bash
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](#)

#### 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 1180

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
Extended-Range VLAN Configuration Guidelines, on page 1175

Where to Go Next

After configuring VLANs, you can configure the following:

• VLAN Trunking Protocol (VTP)
• VLAN trunks
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 1191
- [Layer 2 Interface Modes](#), on page 1188

**Layer 2 Interface Modes**

**Table 130: 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>
FunctionMode

Makestheinterfaceabletoconvertthelinktoatrunklink. Theinterface becomesatrunkinterfaceiftheneighboringinterfaceissettotrunkor
desirablemode. 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

Putstheinterfaceintopermanenttrunkingmodeandnegotiates toconvertthe
neighboringlinkintoatrunklink. Theinterface becomesatrunkinterface
even iftheneighboringinterfaceisnotatrunkinterface.

Switchport nonegotiate

PreventstheinterfacefromgeneratingDTPframes. You can usethiscommand
onlywhentheinterface switchport mode is access or trunk. You must manually
configuretheneighboringinterfaceasatrunkinterface toestablishatrunk
link.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport mode dynamic auto</td>
<td>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.</td>
</tr>
<tr>
<td>switchport mode dynamic desirable</td>
<td>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.</td>
</tr>
<tr>
<td>switchport mode trunk</td>
<td>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.</td>
</tr>
<tr>
<td>switchport nonegotiate</td>
<td>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.</td>
</tr>
</tbody>
</table>

Related Topics

Configuring a Trunk Port, on page 1191
Trunking Modes, on page 1188

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 1193
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 1198

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 1201

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 131: 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 to not 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></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>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the port to be configured for trunking, and enters interface configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configures the interface as a Layer 2 trunk (required only if the interface is a Layer 2 access port or tunnel port or to specify the trunking mode).</td>
</tr>
<tr>
<td>`switchport mode {dynamic {auto</td>
<td>desirable}</td>
</tr>
<tr>
<td></td>
<td>- <strong>dynamic desirable</strong>—Sets the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode.</td>
</tr>
<tr>
<td></td>
<td>- <strong>trunk</strong>—Sets the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Specifies the default VLAN, which is used if the interface stops trunking.</td>
</tr>
<tr>
<td><code>switchport access vlan vlan-id</code></td>
<td></td>
</tr>
</tbody>
</table>
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. `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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface interface-id</code></td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <code>interface gigabitethernet 0/1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>switchport mode trunk</code></td>
<td>Configures the interface as a VLAN trunk port.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# <code>switchport mode trunk</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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch(config)# <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 Trunking VLANs Enabled field of the display.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch# <code>show interfaces gigabitethernet 0/1 switchport</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
--- | ---
Step 7 | copy running-config startup-config
Example: | (Optional) Saves your entries in the configuration file.
Switch# copy running-config startup-config

### Related Topics

- [Allowed VLANS on a Trunk](#), on page 1189

## 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><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Switch&gt; enable</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>Enters global configuration mode.</td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Example:</td>
<td>Selects the trunk port for which VLANs should be pruned, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# interface fastethernet0/1-48</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport trunk pruning vlan {add</td>
</tr>
<tr>
<td></td>
<td>Configures the list of VLANs allowed to be pruned from the trunk.</td>
</tr>
</tbody>
</table>
For explanations about using the add, except, none, and remove keywords, see the command reference for this release.

Separate non-consecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are 2 to 1001. Extended-range VLANs (VLAN IDs 1006 to 4094) cannot be pruned.

VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001.

Step 5  
**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

Step 6  
**Example:**

Switch# show interfaces gigabitethernet 0/1 switchport

Verifies your entries in the Pruning VLANs Enabled field of the display.

Step 7  
**Example:**

Switch# copy running-config startup-config

(Optional) Saves your entries in the configuration file.

**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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable`<br>`Switch> enable` | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Step 2 | `configure terminal`<br>`Switch# configure terminal` | Enters global configuration mode. |
| Step 3 | `interface interface-id`<br>`Switch(config)# interface gigabitethernet 0/2` | Defines the interface that is configured as the IEEE 802.1Q trunk, and enters interface configuration mode. |
| Step 4 | `switchport trunk native vlan vlan-id`<br>`Switch(config-if)# switchport trunk native vlan 12` | Configures the VLAN that is sending and receiving untagged traffic on the trunk port.  
  For `vlan-id`, the range is 1 to 4094. |
| Step 5 | `end`<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| Step 6 | `show interfaces interface-id switchport`<br>`Switch# show interfaces gigabitethernet 0/2 switchport` | Verifies your entries in the **Trunking Native Mode VLAN** field. |
| Step 7 | `copy running-config startup-config`<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |
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

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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Switch&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode on Switch A.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></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**

vtp domain *domain-name*

**Example:**

Switch(config)# vtp domain workdomain

Configures a VTP administrative domain.
The domain name can be 1 to 32 characters.

**Step 4**

vtp mode server

**Example:**

Switch(config)# vtp mode server

Configures Switch A as the VTP server.

**Step 5**

eend

**Example:**

Switch(config)# end

Returns to privileged EXEC mode.

**Step 6**

show vtp status

**Example:**

Switch# show vtp status

Verifies the VTP configuration on both Switch A and Switch B.
In the display, check the *VTP Operating Mode* and the *VTP Domain Name* fields.

**Step 7**

show vlan

**Example:**

Switch# show vlan

Verifies that the VLANs exist in the database on Switch A.

**Step 8**

configure terminal

**Example:**

Switch# configure terminal

Enters global configuration mode.

**Step 9**

interface *interface-id*

**Example:**

Switch(config)# interface fastethernet0/1-48

Defines the interface to be configured as a trunk, and enters interface configuration mode.

**Step 10**

switchport mode trunk

**Example:**

Configures the port as a trunk port.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>Returns to privileged EXEC mode.</strong></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>Verifies the VLAN configuration.</strong></td>
</tr>
<tr>
<td>show interfaces interface-id switchport</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show interfaces gigabitethernet 0/1 switchport</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>Repeat the above steps on Switch A for a second port in the switch.</strong></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>Repeat the above steps on Switch B to configure the trunk ports that connect to the trunk ports configured on Switch A.</strong></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>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.</strong></td>
</tr>
<tr>
<td>show vlan</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# show vlan</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td><strong>Enters global configuration mode on Switch A.</strong></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 17</strong></td>
<td><strong>Defines the interface to set the STP port priority, and enters interface configuration mode.</strong></td>
</tr>
<tr>
<td>interface interface-id</td>
<td></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 18</strong></td>
<td><strong>Assigns the port priority for the VLAN range specified. Enter a port priority value from 0 to 240. Port priority values increment by 16.</strong></td>
</tr>
<tr>
<td>spanning-tree vlan vlan-range port-priority priority-value</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config-if)# spanning-tree vlan 8-10 port-priority 16</td>
<td></td>
</tr>
<tr>
<td><strong>Step 19</strong></td>
<td><strong>Returns to global configuration mode.</strong></td>
</tr>
<tr>
<td>exit</td>
<td></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>exit</code></td>
<td>Defines the interface to set the STP port priority, and enters interface configuration mode.</td>
</tr>
</tbody>
</table>

**Step 20**

`interface interface-id`

**Example:**

```
Switch(config)# interface gigabitethernet 0/2
```

**Step 21**

`spanning-tree vlan vlan-range port-priority priority-value`

**Example:**

```
Switch(config-if)# spanning-tree vlan 3-6 port-priority 16
```

**Step 22**

`end`

**Example:**

```
Switch(config-if)# end
```

**Step 23**

`show running-config`

**Example:**

```
Switch# show running-config
```

**Step 24**

`copy running-config startup-config`

**Example:**

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

---

**Related Topics**

*Network Load Sharing Using STP Priorities*, on page 1190

---

**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: Switch(config-if)# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch(config-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>----------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Repeat Steps 2 through 4 on a second interface in Switch A.</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td><strong>end</strong>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;Switch(config)# end</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td><strong>show running-config</strong>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;Switch# show running-config</td>
</tr>
<tr>
<td><strong>9</strong></td>
<td><strong>show vlan</strong>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;Switch# show vlan</td>
</tr>
<tr>
<td><strong>10</strong></td>
<td><strong>configure terminal</strong>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;Switch# configure terminal</td>
</tr>
<tr>
<td><strong>11</strong></td>
<td><strong>interface</strong> <em>interface-id</em>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;Switch(config)# interface gigabitethernet 0/1</td>
</tr>
<tr>
<td><strong>12</strong></td>
<td><strong>spanning-tree vlan</strong> <em>vlan-range</em> <strong>cost</strong> <em>cost-value</em>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;Switch(config-if)# spanning-tree vlan 2-4 cost 30</td>
</tr>
<tr>
<td><strong>13</strong></td>
<td><strong>end</strong>  &lt;br&gt;<strong>Example:</strong>  &lt;br&gt;Switch(config-if)# end</td>
</tr>
<tr>
<td><strong>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>
</tbody>
</table>
## 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 trunking.

Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config-if)# 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

---

**Related Topics**

- Network Load Sharing Using STP Path Cost, on page 1190
Where to Go Next

After configuring VLAN trunks, you can configure the following:

- VLANs

Additional References

<table>
<thead>
<tr>
<th>Standards and RFCs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard/RFC</strong></td>
</tr>
<tr>
<td><strong>Title</strong></td>
</tr>
<tr>
<td>——</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MIBs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MIB</strong></td>
</tr>
<tr>
<td>All the supported MIBs for this release.</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>
</tbody>
</table>

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.

<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 VLAN Trunks

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Configuring Voice VLANs

- Finding Feature Information, on page 1207
- Prerequisites for Voice VLANs, on page 1207
- Restrictions for Voice VLANs, on page 1208
- Information About Voice VLAN, on page 1208
- How to Configure Voice VLAN, on page 1210
- Monitoring Voice VLAN, on page 1212
- Configuration Examples, on page 1212
- Where to Go Next, on page 1213
- Additional References, on page 1213
- Feature History and Information for Voice VLAN, on page 1214

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)

Note: 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 1212
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\{vlan-id | 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

**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>interface interface-id</td>
<td>Specifies the interface connected to the phone, and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config)# interface gigabitethernet 0/1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>mls qos trust cos</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:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch(config-if)# mls qos trust cos</td>
<td>Note: Before configuring the port trust state, you must first globally enable QoS by using the mls qos global configuration command.</td>
</tr>
<tr>
<td>5</td>
<td>switchport voice {vlan{vlan-id</td>
<td>dot1p</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>• vlan-id—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>Switch(config-if)# switchport voice vlan dot1p</td>
<td>• dot1p—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>
### 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 1208

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 the 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 Voice VLAN

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Release 15.2(5)E</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
Important Notice

• Disclaimer, on page 1215
• Statement 361—VoIP and Emergency Calling Services do not Function if Power Fails, on page 1215
• Statement 1071—Warning Definition, on page 1217

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>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>
</tr>
<tr>
<td>Language</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>Scots/Gaelic</td>
</tr>
<tr>
<td>French</td>
</tr>
<tr>
<td>German</td>
</tr>
<tr>
<td>Italian</td>
</tr>
<tr>
<td>Norwegian</td>
</tr>
<tr>
<td>Portuguese</td>
</tr>
<tr>
<td>Spanish</td>
</tr>
</tbody>
</table>
Warning!

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 hozzáérhessen a VoIP és a segélyhívó szolgáltatásokhoz. 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，以便重新获得进入 VoIP 与紧急呼叫服务的权限。在美国，紧急呼叫号码是 911。您必须知道本国的紧急呼叫号码。

警告
电源故障或停電の場合、ボイスオーバーアイページ(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。

Software Configuration Guide, Cisco IOS Release 15.2(6)E (Catalyst 2960-L Switches)
<table>
<thead>
<tr>
<th>Language</th>
<th>Important Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Varoitus</strong></td>
<td><strong>TÄRKEITÄ TURVALLISUUSOHJEITA</strong></td>
</tr>
<tr>
<td></td>
<td>Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuskien yleisiihntäihin. Turvallisuusvaroitusten käännöksset löytyvät laitteesten mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta lopussa näkyvien lausuntonumeroiden avulla.</td>
</tr>
<tr>
<td><strong>Attention</strong></td>
<td><strong>IMPORTANTES INFORMATIONS DE SÉCURITÉ</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Warnung</strong></td>
<td><strong>WICHTIGE SICHERHEITSHINWEISE</strong></td>
</tr>
<tr>
<td><strong>Avvertenza</strong></td>
<td><strong>IMPORTANTI ISTRUZIONI SULLA SICUREZZA</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Advarsel</strong></td>
<td><strong>VIKTIGE SIKKERHETSINSTRUKSJONER</strong></td>
</tr>
<tr>
<td></td>
<td>Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. For 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 oversettelsen i de oversatte sikkerhetsadvarslerne som fulgte med denne enheten.</td>
</tr>
<tr>
<td>Aviso</td>
<td>INSTRUÇÕES IMPORTANTES DE SEGURANÇA .</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------</td>
</tr>
</tbody>
</table>
|       | 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 |

<table>
<thead>
<tr>
<th>¡Advertencia!</th>
<th>INSTRUCCIONES IMPORTANTES DE SEGURIDAD</th>
</tr>
</thead>
</table>
|              | 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 |

<table>
<thead>
<tr>
<th>Varning!</th>
<th>VIKTIGA SÄKERHETSANVISNINGAR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SPARA DESSA ANVISNINGAR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Figyelem</th>
<th>FONTOS BIZTONSÁGI ELOÍRÁSOK</th>
</tr>
</thead>
</table>
|          | Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejt a helyzetben van. Mielőtt bármely berendezésen munkát végezte, legyen figyellemmel az elektromos áramkörek okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplő figyelmeztetések fordítása a készülékhez mellékelh biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján kereshető meg.
|          | ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT! |

| Предупреждение | Для обеспечения соответствия требованиям по предельным значениям облучению радиочастотами (РЧ) антенны данного устройства должны располагаться на расстоянии не ближе 2 м от пользователей. |

| 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。电源恢复正常之后，您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) サービスと緊急電話サービスは機能しません。電源の回復後、VoIP と緊急電話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。米国内の緊急電話番号は 911 です。お住まいの地域の緊急電話番号をあらかじめ調べておいてください。 |