# INDEX

## A

AAA down policy, NAC Layer 2 IP validation 1-11  
abbreviating commands 2-4  
ABRs 37-24  
AC (command switch) 5-11  
access-class command 33-19  
access control entries  
  See ACEs  
access control entry (ACE) 40-3  
access-denied response, VMPS 13-28  
access groups  
  applying IPv4 ACLs to interfaces 33-20  
  Layer 2 33-20  
  Layer 3 33-20  
accessing  
  clusters, switch 5-14  
  command switches 5-12  
  member switches 5-14  
  switch clusters 5-14  
access lists  
  See ACLs  
access ports  
  and Layer 2 protocol tunneling 16-11  
  defined 11-3  
  in switch clusters 5-10  
access template 7-1  
accounting  
  with 802.1x 9-52  
  with IEEE 802.1x 9-16  
  with RADIUS 8-34  
  with TACACS+ 8-11, 8-17  
A CEs  
  and QoS 34-8  
  defined 33-2  
  Ethernet 33-2  
  IP 33-2  
ACLs  
  ACEs 33-2  
  any keyword 33-12  
  applying  
    on bridged packets 33-38  
    on multicast packets 33-40  
    on routed packets 33-39  
    on switched packets 33-38  
    time ranges to 33-16  
    to an interface 33-19, 40-7  
    to IPv6 interfaces 40-7  
    to QoS 34-8  
  classifying traffic for QoS 34-48  
  comments in 33-18  
  compiling 33-22  
  defined 33-1, 33-7  
  examples of 33-22, 34-48  
  extended IP, configuring for QoS classification 34-49  
  extended IPv4  
    creating 33-10  
    matching criteria 33-7  
  hardware and software handling 33-21  
  host keyword 33-12
ACLs (continued)

IP
creating 33-7
fragments and QoS guidelines 34-38
implicit deny 33-9, 33-13, 33-15
implicit masks 33-9
matching criteria 33-7
undefined 33-20

IPv4
applying to interfaces 33-19
creating 33-7
matching criteria 33-7
named 33-14
numbers 33-8
terminal lines, setting on 33-19
unsupported features 33-6

IPv6
applying to interfaces 40-7
configuring 40-3, 40-4
displaying 40-8
interactions with other features 40-4
limitations 40-3
matching criteria 40-3
named 40-3
precedence of 40-2
supported 40-2
unsupported features 40-3
Layer 4 information in 33-37
logging messages 33-8
MAC extended 33-27, 34-50
matching 33-7, 33-20, 40-3
monitoring 33-41, 40-8
named, IPv4 33-14
named, IPv6 40-3
names 40-4
number per QoS class map 34-38
port 33-2, 40-1
precedence of 33-3
QoS 34-8, 34-48

ACLs (continued)
resequencing entries 33-14
router 33-2, 40-1
router ACLs and VLAN map configuration guidelines 33-37
standard IP, configuring for QoS classification 34-48
standard IPv4
creating 33-9
matching criteria 33-7
support for 1-9
support in hardware 33-21
time ranges 33-16
types supported 33-2
unsupported features, IPv4 33-6
unsupported features, IPv6 40-3
using router ACLs with VLAN maps 33-36
VLAN maps
configuration guidelines 33-30
configuring 33-29
active link 19-4, 19-5, 19-6
active links 19-2
active router 41-1
active traffic monitoring, IP SLAs 42-1
address aliasing 22-2
addresses
displaying the MAC address table 6-30
dynamic
accelerated aging 26-8
changing the aging time 6-21
default aging 26-8
defined 6-19
learning 6-20
removing 6-22
IPv6 38-2
MAC, discovering 6-30
multicast
group address range 45-3
STP address management 26-8
addresses (continued)
  static
    adding and removing 6-26
    defined 6-19
address resolution 6-30, 37-8
Address Resolution Protocol
  See ARP
adjacency tables, with CEF 37-88
administrative distances
  defined 37-101
  OSPF 37-31
  routing protocol defaults 37-90
advertisements
  CDP 24-1
  LLDP 25-1, 25-2
  RIP 37-19
  VTP 13-19, 14-3, 14-4
aggregatable global unicast addresses 38-3
aggregate addresses, BGP 37-58
aggregated ports
  See EtherChannel
aggregate policers 34-64
aggregate policing 1-12
aging, accelerating 26-8
aging time
  accelerated
    for MSTP 17-24
    for STP 26-8, 26-21
  MAC address table 6-21
  maximum
    for MSTP 17-25
    for STP 26-21, 26-22
alarms, RMON 29-4
allowed-VLAN list 13-22
application engines, redirecting traffic to area border routers
  See ABRs
area routing
  IS-IS 37-63
  ISO IGRP 37-63
ARP
  configuring 37-9
  defined 1-6, 6-30, 37-8
  encapsulation 37-9
  static cache configuration 37-9
  table
    address resolution 6-30
    managing 6-30
ASBRs 37-24
AS-path filters, BGP 37-52
asymmetrical links, and IEEE 802.1Q tunneling 16-4
attributes, RADIUS
  vendor-proprietary 8-37
  vendor-specific 8-35
attribute-value pairs 9-13, 9-16, 9-21, 9-22
authentication
  EIGRP 37-38
  HSRP 41-10
  local mode with AAA 8-44
  NTP associations 6-5
  open1x 9-31
  RADIUS
    key 8-27
    login 8-29
  TACACS+
    defined 8-11
    key 8-13
    login 8-14
  See also port-based authentication
authentication compatibility with Catalyst 6000 switches 9-9
authentication failed VLAN
  See restricted VLAN
authentication keys, and routing protocols 37-102
authentication manager

CLI commands 9-10
compatibility with older 802.1x CLI commands 9-10 to ??
overview 9-8

authorization

with RADIUS 8-33
with TACACS+ 8-11, 8-16

authorized ports with IEEE 802.1x 9-11
autoconfiguration 3-3
auto enablement 9-33
automatic discovery

considerations

beyond a noncandidate device 5-8
brand new switches 5-10
connectivity 5-5
different VLANs 5-7
management VLANs 5-8
non-CDP-capable devices 5-7
noncluster-capable devices 5-7
routed ports 5-9
in switch clusters 5-5
See also CDP

automatic QoS

See QoS

automatic recovery, clusters 5-11
See also HSRP

auto-MDIX

configuring 11-21
described 11-21

autonegotiation

duplex mode 1-3
interface configuration guidelines 11-18
mismatches 48-11

autonomous system boundary routers

See ASBRs

autonomous systems, in BGP 37-46
Auto-QoS video devices 1-13

Auto-RP, described 45-6
autosensing, port speed 1-3
autostate exclude 11-5
auxiliary VLAN

See voice VLAN
availability, features 1-7

B

BackboneFast

described 18-5
disabling 18-15
enabling 18-14
support for 1-7

backup interfaces

See Flex Links

backup links 19-2

backup static routing, configuring 43-12

banners

configuring

login 6-19
message-of-the-day login 6-18
default configuration 6-17
when displayed 6-17

Berkeley r-tools replacement 8-56

BGP

aggregate addresses 37-58
aggregate routes, configuring 37-58
CIDR 37-58
clear commands 37-61
community filtering 37-55
configuring neighbors 37-56
default configuration 37-43
described 37-42
enabling 37-46
monitoring 37-61
multipath support 37-50
neighbors, types of 37-46
path selection 37-50
BGP (continued)

peers, configuring 37-56
prefix filtering 37-54
resetting sessions 37-49
route dampening 37-60
route maps 37-52
route reflectors 37-59
routing domain confederation 37-59
routing session with multi-VRF CE 37-82
show commands 37-61
supernets 37-58
support for 1-13
Version 4 37-43

binding cluster group and HSRP group 41-12

binding database
address, DHCP server
See DHCP, Cisco IOS server database
DHCP snooping
See DHCP snooping binding database

bindings
address, Cisco IOS DHCP server 20-7
DHCP snooping database 20-8
IP source guard 20-17

binding table, DHCP snooping
See DHCP snooping binding database

blocking packets 23-8
Boolean expressions in tracked lists 43-4
booting
boot loader, function of 3-2
boot process 3-2
manually 3-20
specific image 3-21

boot loader
accessing 3-22
described 3-2
environment variables 3-22
prompt 3-22
trap-door mechanism 3-2
bootstrap router (BSR), described 45-7

Border Gateway Protocol
See BGP

BPDU
error-disabled state 18-3
filtering 18-3
RSTP format 17-12

BPDU filtering
described 18-3
disabling 18-13
enabling 18-13
support for 1-8

BPDU guard
described 18-2
disabling 18-12
enabling 18-12
support for 1-8

bridged packets, ACLs on 33-38
bridge groups
See fallback bridging
bridge protocol data unit
See BPDU

broadcast flooding 37-16
broadcast packets
directed 37-13
flooded 37-13

broadcast storm-control command 23-4
broadcast storms 23-2, 37-13

C

cables, monitoring for unidirectional links 27-1
candidate switch
automatic discovery 5-5
defined 5-3
requirements 5-3
See also command switch, cluster standby group, and member switch
Catalyst 6000 switches
authentication compatibility 9-9
<table>
<thead>
<tr>
<th>CA trustpoint</th>
<th>configuring [8-53]</th>
<th>defined [8-50]</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP</td>
<td>and trusted boundary [34-44]</td>
<td>automatic discovery in switch clusters [5-5]</td>
</tr>
<tr>
<td></td>
<td>configuring [24-2]</td>
<td>default configuration [24-2]</td>
</tr>
<tr>
<td></td>
<td>defined with LLDP [25-1]</td>
<td>described [24-1]</td>
</tr>
<tr>
<td></td>
<td>disabling for routing device [24-4]</td>
<td>enabling and disabling</td>
</tr>
<tr>
<td></td>
<td>on an interface [24-4]</td>
<td>on a switch [24-4]</td>
</tr>
<tr>
<td></td>
<td>Layer 2 protocol tunneling [16-8]</td>
<td>monitoring [24-5]</td>
</tr>
<tr>
<td></td>
<td>overview [24-1]</td>
<td>power negotiation extensions [11-7]</td>
</tr>
<tr>
<td></td>
<td>support for [1-6]</td>
<td>transmission timer and holdtime, setting [24-3]</td>
</tr>
<tr>
<td></td>
<td>updates [24-3]</td>
<td></td>
</tr>
<tr>
<td>CEF</td>
<td>defined [37-88]</td>
<td>enabling [37-88]</td>
</tr>
<tr>
<td></td>
<td>IPv6 [38-18]</td>
<td></td>
</tr>
<tr>
<td>CGMP</td>
<td>as IGMP snooping learning method [22-9]</td>
<td>clearing cached group entries [45-62]</td>
</tr>
<tr>
<td></td>
<td>enabling server support [45-44]</td>
<td>joining multicast group [22-3]</td>
</tr>
<tr>
<td></td>
<td>overview [45-9]</td>
<td>server support only [45-9]</td>
</tr>
<tr>
<td></td>
<td>switch support of [1-4]</td>
<td></td>
</tr>
<tr>
<td>CIDR [37-58]</td>
<td>CipherSuites [8-51]</td>
<td></td>
</tr>
<tr>
<td>Cisco 7960 IP Phone [12-1]</td>
<td>Cisco Discovery Protocol</td>
<td>See CDP</td>
</tr>
<tr>
<td></td>
<td>Cisco Express Forwarding</td>
<td>See CEF</td>
</tr>
<tr>
<td></td>
<td>Cisco Group Management Protocol</td>
<td>See CGMP</td>
</tr>
<tr>
<td></td>
<td>Cisco intelligent power management [11-7]</td>
<td>Cisco IOS DHCP server</td>
</tr>
<tr>
<td></td>
<td>See DHCP, Cisco IOS DHCP server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS File System</td>
<td>See IFS</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS IP SLAs [42-1]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Redundant Power System 2300</td>
<td>configuring [11-29]</td>
</tr>
<tr>
<td></td>
<td>managing [11-29]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Secure ACS</td>
<td>attribute-value pairs for downloadable ACLs [9-22]</td>
</tr>
<tr>
<td></td>
<td>attribute-value pairs for redirect URL [9-21]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Secure ACS configuration guide [9-63]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CiscoWorks 2000 [1-5, 31-4]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CISP [9-33]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIST regional root</td>
<td>See MSTP</td>
</tr>
<tr>
<td></td>
<td>See MSTP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>civic location [25-3]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>classless interdomain routing</td>
<td>See CIDR</td>
</tr>
<tr>
<td></td>
<td>classless routing [37-6]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>class maps for QoS</td>
<td>configuring [34-51]</td>
</tr>
<tr>
<td></td>
<td>described [34-8]</td>
<td>displaying [34-84]</td>
</tr>
<tr>
<td></td>
<td>class of service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See CoS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clearing interfaces [11-32]</td>
<td></td>
</tr>
<tr>
<td>CLI</td>
<td>abbreviating commands [2-4]</td>
<td>command modes [2-1]</td>
</tr>
<tr>
<td></td>
<td>configuration logging [2-5]</td>
<td>described [1-5]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
INDEX

CLI (continued)
- editing features
  - enabling and disabling 2-7
  - keystroke editing 2-8
  - wrapped lines 2-9
- error messages 2-5
- filtering command output 2-10
- getting help 2-3
- history
  - changing the buffer size 2-6
  - described 2-6
  - disabling 2-7
  - recalling commands 2-6
- managing clusters 5-16
- no and default forms of commands 2-4

Clusters, switch (continued)
- host names 5-14
- IP addresses 5-14
- LRE profiles 5-15
- passwords 5-14
- RADIUS 5-15
- SNMP 5-15, 5-16
- TACACS+ 5-15
See also candidate switch, command switch, cluster standby group, member switch, and standby command switch

Cluster standby group
- and HSRP group 41-12
- automatic recovery 5-13
- considerations 5-12
- defined 5-2
- requirements 5-3
- virtual IP address 5-12
See also HSRP

CNS 1-5
Configuration Engine
- configID, deviceID, hostname 4-3
- configuration service 4-2
- described 4-1
- event service 4-3
- embedded agents
  - described 4-5
  - enabling automated configuration 4-6
  - enabling configuration agent 4-9
  - enabling event agent 4-7
- management functions 1-5

CoA Request Commands 8-24

Coarse Wave Division Multiplexer
- See CWDM SFPs

Command-line interface
- See CLI

Command modes 2-1
configuration conflicts, recovering from lost member connectivity
configuration examples, network
configuration files
configuration guidelines, multi-VRF CE
configuration logger
configuration logging
configuration replacement
configuration rollback
commands abbreviating
commands, setting privilege levels
command switch
accessing
active (AC)
configuration conflicts
defined
passive (PC)
priority
recovery
from command-switch failure
from lost member connectivity
redundant
replacing
with another switch
with cluster member
requirements
standby (SC)
See also candidate switch, cluster standby group, member switch, and standby command switch
community list, BGP
community ports
community strings
configuring
for cluster switches
in clusters
overview
SNMP
community VLANs
compatibility, feature
config.text
configurable leave timer, IGMP
configuration, initial
defaults
Express Setup
configuration changes, logging
configuration conflicts, recovering from lost member connectivity
configuration examples, network
configuration files
configuration guidelines, multi-VRF CE
configuration logger
configuration logging
configuration replacement
configuration rollback
commands abbreviating
commands, setting privilege levels
command switch
accessing
active (AC)
configuration conflicts
defined
passive (PC)
priority
recovery
from command-switch failure
from lost member connectivity
redundant
replacing
with another switch
with cluster member
requirements
standby (SC)
See also candidate switch, cluster standby group, member switch, and standby command switch
community list, BGP
community ports
community strings
configuring
for cluster switches
in clusters
overview
SNMP
community VLANs
compatibility, feature
config.text
configurable leave timer, IGMP
configuration, initial
defaults
Express Setup
configuration changes, logging
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
</table>

| configuration settings, saving | 3-16 |
| configure terminal command | 11-11 |
| configuring 802.1x user distribution | 9-59 |
| configuring port-based authentication violation modes | 9-41 to 9-42 |
| configuring small-frame arrival rate | 23-5 |
| config-vlan mode | 2-2 |
| conflicts, configuration | 48-11 |
| connections, secure remote | 8-45 |
| connectivity problems | 48-13, 48-14, 48-16 |
| consistency checks in VTP Version 2 | 14-4 |
| console port, connecting to | 2-10 |
| content-routing technology  |  |
| See WCCP |
| control protocol, IP SLAs | 42-4 |
| corrupted software, recovery steps with Xmodem | 48-2 |
| CoS in Layer 2 frames | 34-2 |
| override priority | 12-7 |
| trust priority | 12-7 |
| CoS input queue threshold map for QoS | 34-17 |
| CoS output queue threshold map for QoS | 34-19 |
| CoS-to-DSCP map for QoS | 34-67 |
| counters, clearing interface | 11-32 |
| CPU utilization, troubleshooting | 48-25 |
| crashinfo file | 48-23 |
| critical authentication, IEEE 802.1x | 9-56 |
| critical VLAN | 9-25 |
| cryptographic software image  |  |
| Kerberos | 8-39 |
| SSH | 8-45 |
| SSL | 8-49 |
| customer edge devices | 37-73 |
| customjzeable web pages, web-based authentication | 10-6 |
| CWDM SFPs | 1-26 |

### D

| DACL | See downloadable ACL |
| daylight saving time | 6-13 |
| debugging  |  |
| enabling all system diagnostics | 48-20 |
| enabling for a specific feature | 48-19 |
| redirecting error message output | 48-20 |
| using commands | 48-19 |
| default commands | 2-4 |
| default configuration |  |
| 802.1x | 9-36 |
| auto-QoS | 34-21 |
| banners | 6-17 |
| BGP | 37-43 |
| booting | 3-19 |
| CDP | 24-2 |
| DHCP | 20-10 |
| DHCP option 82 | 20-10 |
| DHCP snooping | 20-10 |
| DHCP snooping binding database | 20-10 |
| DNS | 6-16 |
| dynamic ARP inspection | 21-5 |
| EIGRP | 37-35 |
| EtherChannel | 35-10 |
| Ethernet interfaces | 11-15 |
| fallback bridging | 47-3 |
| Flex Links | 19-8 |
| HSRP | 41-5 |
| IEEE 802.1Q tunneling | 16-4 |
| IGMP | 45-39 |
| IGMP filtering | 22-26 |
| IGMP snooping | 22-27, 39-6 |
| IGMP throttling | 22-26 |
| initial switch information | 3-3 |
| IP addressing, IP routing | 37-4 |
| IP multicast routing | 45-10 |
| IP SLAs | 42-6 |
default configuration (continued)

IP source guard 20-19
IPv6 38-10
IS-IS 37-64
Layer 2 interfaces 11-15
Layer 2 protocol tunneling 16-11
LLDP 25-5
MAC address table 6-21
MAC address-table move update 19-8
MSDP 46-4
MSTP 17-15
multi-VRF CE 37-75
MVR 22-20
NTP 6-4
optional spanning-tree configuration 18-10
OSPF 37-25
password and privilege level 8-3
PIM 45-10
private VLANs 15-6
RADIUS 8-26
RIP 37-19
RMON 29-3
RSPAN 28-10
SDM template 7-3
SNMP 31-6
SPAN 28-10
SSL 8-52
standard QoS 34-35
STP 26-11
system message logging 30-3
system name and prompt 6-15
TACACS+ 8-13
UDLD 27-4
VLAN, Layer 2 Ethernet interfaces 13-19
VLANs 13-7
VMPS 13-29
voice VLAN 12-3
VTP 14-7
WCCP 44-5
default gateway 3-16, 37-11
default networks 37-91
default router preference
See DRP
default routes 37-91
default routing 37-2
default web-based authentication configuration
802.1X 10-9
deleting VLANs 13-9
denial-of-service attack 23-2
description command 11-25
designing your network, examples 1-19
destination addresses
in IPv4 ACLs 33-11
in IPv6 ACLs 40-5
destination-IP address-based forwarding, EtherChannel 35-8
destination-MAC address forwarding, EtherChannel 35-8
detecting indirect link failures, STP 18-5
device 8-24
device discovery protocol 24-1, 25-1
device manager
benefits 1-2
described 1-2, 1-5
in-band management 1-6
upgrading a switch 8-24
DHCP
Cisco IOS server database
configuring 20-15
default configuration 20-10
described 20-7
DHCP for IPv6
See DHCPv6
enabling
relay agent 20-11
DHCP-based autoconfiguration
  client request message exchange 3-4
  configuring
    client side 3-4
    DNS 3-8
    relay device 3-8
    server side 3-7
    TFTP server 3-8
  example 3-10
  lease options
    for IP address information 3-7
    for receiving the configuration file 3-7
  overview 3-3
  relationship to BOOTP 3-4
  relay support 1-5, 1-14
  support for 1-5

DHCP-based autoconfiguration and image update
  configuring 3-12 to 3-15
  understanding 3-5 to 3-6

DHCP binding database
  See DHCP snooping binding database

DHCP binding table
  See DHCP snooping binding database

DHCP object tracking, configuring primary interface 43-10

DHCP option 82
  circuit ID suboption 20-5
  configuration guidelines 20-10
  default configuration 20-10
  displaying 20-16
  forwarding address, specifying 20-12
  helper address 20-12
  overview 20-4
  packet format, suboption
    circuit ID 20-5
    remote ID 20-5
  remote ID suboption 20-5

DHCP server port-based address allocation
  configuration guidelines 20-27
  default configuration 20-27
  described 20-27
  displaying 20-30
  enabling 20-28
  reserved addresses 20-28

DHCP server port-based address assignment
  support for 1-6

DHCP snooping
  accepting untrusted packets form edge switch 20-3, 20-13
  and private VLANs 20-15
  binding database
    See DHCP snooping binding database
  configuration guidelines 20-10
  default configuration 20-10
  displaying binding tables 20-16
  message exchange process 20-4
  option 82 data insertion 20-4
  trusted interface 20-2
  untrusted interface 20-2
  untrusted messages 20-2

DHCP snooping binding database
  adding bindings 20-15
  binding file
    format 20-8
    location 20-8
    bindings 20-8
  clearing agent statistics 20-16
  configuration guidelines 20-11
  configuring 20-15
  default configuration 20-10
  deleting
    binding file 20-16
    bindings 20-16
    database agent 20-16
  described 20-8
DHCP snooping binding database (continued)
  displaying 20-16
  binding entries 20-16
  status and statistics 20-16
enabling 20-15
entry 20-8
renewing database 20-16
resetting
  delay value 20-16
  timeout value 20-16
DHCP snooping binding table
  See DHCP snooping binding database
DHCPv6
  configuration guidelines 38-15
  default configuration 38-15
  described 38-6
  enabling client function 38-17
  enabling DHCPv6 server function 38-15
  support for 1-14
Differentiated Services architecture, QoS 34-2
Differentiated Services Code Point 34-2
Diffusing Update Algorithm (DUAL) 37-33
directed unicast requests 1-6
directories
  changing B-3
  creating and removing B-4
  displaying the working B-3
discovery, clusters
  See automatic discovery
Distance Vector Multicast Routing Protocol
  See DVMRP
distance-vector protocols 37-3
distribute-list command 37-101
DNS
  and DHCP-based autoconfiguration 3-8
  default configuration 6-16
  displaying the configuration 6-17
  in IPv6 38-4
  overview 6-15
DNS (continued)
  setting up 6-16
  support for 1-5
DNS-based SSM mapping 45-18, 45-20
domain names
  DNS 6-15
  VTP 14-8
Domain Name System
  See DNS
domains, ISO IGRP routing 37-63
dot1q-tunnel switchport mode 13-17
double-tagged packets
  IEEE 802.1Q tunneling 16-2
  Layer 2 protocol tunneling 16-10
downloadable ACL 9-20, 9-22, 9-63
downloading
  configuration files
    preparing B-10, B-13, B-16
    reasons for B-8
    using FTP B-13
    using RCP B-17
    using TFTP B-11
  image files
    deleting old image B-28
    preparing B-26, B-30, B-34
    reasons for B-24
    using CMS 1-2
    using FTP B-31
    using HTTP 1-2, B-24
    using RCP B-35
    using TFTP B-27
    using the device manager or Network Assistant B-24
drop threshold for Layer 2 protocol packets 16-11
DRP
  configuring 38-13
  described 38-5
IPv6 38-5
  support for 1-14
DSCP 1-12, 34-2
DSCP input queue threshold map for QoS 34-17
DSCP output queue threshold map for QoS 34-19
DSCP-to-CoS map for QoS 34-70
DSCP-to-DSCP-mutation map for QoS 34-71
DSCP transparency 34-45
DTP 1-8, 13-17
dual-action detection 35-5
DUAL finite state machine, EIGRP 37-34
dual IPv4 and IPv6 templates 7-2, 38-6
dual protocol stacks
IPv4 and IPv6 38-6
SDM templates supporting 38-6
dual-purpose uplinks
defined 11-6
LEDs 11-6
link selection 11-6, 11-17
setting the type 11-17
DVMRP
autosummarization
configuring a summary address 45-58
disabling 45-60
connecting PIM domain to DVMRP router 45-51
enabling unicast routing 45-54
interoperability
with Cisco devices 45-49
with Cisco IOS software 45-9
mrinfo requests, responding to 45-53
neighbors
advertising the default route to 45-52
discovery with Probe messages 45-49
displaying information 45-53
prevent peering with nonpruning 45-56
rejecting nonpruning 45-55
overview 45-9
DVRMP (continued)
routes
adding a metric offset 45-60
advertising all 45-60
advertising the default route to neighbors 45-52
caching DVMRP routes learned in report messages 45-54
changing the threshold for syslog messages 45-57
deleting 45-62
displaying 45-62
favoring one over another 45-60
limiting the number injected into MBONE 45-57
limiting unicast route advertisements 45-49
routing table 45-9
source distribution tree, building 45-9
support for 1-14
tunnels
configuring 45-51
displaying neighbor information 45-53
dynamic access ports
dynamic ARP inspection
ARP cache poisoning 21-1
ARP requests, described 21-1
ARP spoofing attack 21-1
clearing
log buffer 21-16
statistics 21-16
configuration guidelines 21-6
configuring
ACLs for non-DHCP environments 21-9
in DHCP environments 21-7
log buffer 21-13
rate limit for incoming ARP packets 21-4, 21-11
default configuration 21-5
dynamic ARP inspection (continued)
  denial-of-service attacks, preventing 21-11
  described 21-1
  DHCP snooping binding database 21-2
  displaying
    ARP ACLs 21-15
    configuration and operating state 21-15
    log buffer 21-16
    statistics 21-16
    trust state and rate limit 21-15
  error-disabled state for exceeding rate limit 21-4
  function of 21-2
  interface trust states 21-3
  log buffer
    clearing 21-16
    configuring 21-13
    displaying 21-16
  logging of dropped packets, described 21-4
  man-in-the-middle attack, described 21-2
  network security issues and interface trust states 21-3
  priority of ARP ACLs and DHCP snooping entries 21-4
  rate limiting of ARP packets
    configuring 21-11
    described 21-4
    error-disabled state 21-4
  statistics
    clearing 21-16
    displaying 21-16
  validation checks, performing 21-12
  dynamic auto trunking mode 13-17
  dynamic desirable trunking mode 13-17
Dynamic Host Configuration Protocol
  See DHCP-based autoconfiguration
  dynamic port VLAN membership
    described 13-29
    reconfirming 13-31, 13-32
    troubleshooting 13-33
    types of connections 13-31
dynamic routing 37-3
  ISO CLNS 37-62
  Dynamic Trunking Protocol
    See DTP
E
  EBGP 37-41
  editing features
    enabling and disabling 2-7
    keystrokes used 2-8
    wrapped lines 2-9
  EEM 3.2 32-5
  EIGRP
    authentication 37-38
    components 37-34
    configuring 37-37
    default configuration 37-35
    definition 37-33
    interface parameters, configuring 37-38
    monitoring 37-41
    stub routing 37-39
  ELIN location 25-3
  embedded event manager
    3.2 32-5
    actions 32-4
    configuring 32-1, 32-5
    displaying information 32-7
    environmental variables 32-4
    event detectors 32-2
    policies 32-4
    registering and defining an applet 32-6
    registering and defining a TCL script 32-6
    understanding 32-1
  enable password 8-4
  enable secret password 8-4
  encryption, CipherSuite 8-51
  encryption for passwords 8-4
Enhanced IGRP

See EIGRP

enhanced object tracking
  backup static routing 43-12
  commands 43-1
defined 43-1
DHCP primary interface 43-10
HSRP 43-7
IP routing state 43-2
IP SLAs 43-9
line-protocol state 43-2
network monitoring with IP SLAs 43-11
routing policy, configuring 43-12
static route primary interface 43-10
tracked lists 43-3
enhanced object tracking static routing 43-10
environmental variables, embedded event manager 32-4
environment variables, function of 3-23
equal-cost routing 1-14, 37-89
error-disabled state, BPDU 18-3
error messages during command entry 2-5
EtherChannel
  automatic creation of 35-4, 35-6
  channel groups
    binding physical and logical interfaces 35-3
    numbering of 35-3
configuration guidelines 35-10
configuring
  Layer 2 interfaces 35-11
  Layer 3 physical interfaces 35-14
  Layer 3 port-channel logical interfaces 35-13
default configuration 35-10
described 35-2
displaying status 35-20
forwarding methods 35-7, 35-16
IEEE 802.3ad, described 35-6
interaction
  with STP 35-10
  with VLANs 35-11
EtherChannel (continued)

LACP
  described 35-6
displaying status 35-20
hot-standby ports 35-18
interaction with other features 35-7
modes 35-6
port priority 35-19
system priority 35-19
Layer 3 interface 37-3
load balancing 35-7, 35-16
logical interfaces, described 35-3
PAgP
  aggregate-port learners 35-17
  compatibility with Catalyst 1900 35-17
described 35-4
displaying status 35-20
interaction with other features 35-6
interaction with virtual switches 35-5
learn method and priority configuration 35-17
modes 35-5
support for 1-4
  with dual-action detection 35-5
port-channel interfaces
  described 35-3
  numbering of 35-3
port groups 11-6
support for 1-4
EtherChannel guard
  described 18-7
disabling 18-15
enabling 18-15
Ethernet VLANs
  adding 13-8
defaults and ranges 13-7
modifying 13-8
EUI 38-4
event detectors, embedded event manager 32-2
events, RMON 29-4
examples
  network configuration  1-19
expedite queue for QoS  34-83
Express Setup  1-2
  See also getting started guide
extended crashinfo file  48-23
extended-range VLANs
  configuration guidelines  13-11
  configuring  13-11
  creating  13-12
  creating with an internal VLAN ID  13-13
  defined  13-1
extended system ID
  MSTP  17-18
  STP  26-4, 26-14
extended universal identifier
  See EUI
Extensible Authentication Protocol over LAN  9-1
external BGP
  See EIGRP
external neighbors, BGP  37-46

F
fa0 interface  1-6
fallback bridging
  and protected ports  47-4
  bridge groups
    creating  47-4
    described  47-1
    displaying  47-10
    function of  47-2
    number supported  47-4
    removing  47-4
  bridge table
    clearing  47-10
    displaying  47-10
  configuration guidelines  47-3
  connecting interfaces with  11-10
fallback bridging (continued)
  default configuration  47-3
  described  47-1
  frame forwarding
    flooding packets  47-2
    forwarding packets  47-2
  overview  47-1
  protocol, unsupported  47-3
  STP
    disabling on an interface  47-9
    forward-delay interval  47-8
    hello BPDU interval  47-8
    interface priority  47-6
    maximum-idle interval  47-9
    path cost  47-7
    VLAN-bridge spanning-tree priority  47-5
    VLAN-bridge STP  47-2
  support for  1-14
  SVIs and routed ports  47-1
  unsupported protocols  47-3
  VLAN-bridge STP  26-10
Fast Convergence  19-3
  features, incompatible  23-12
FIB  37-88
  fiber-optic, detecting unidirectional links  27-1
files
  basic crashinfo
    description  48-23
    location  48-23
  copying  B-4
  crashinfo, description  48-23
  deleting  B-5
  displaying the contents of  B-7
  extended crashinfo
    description  48-23
    location  48-23
files (continued)

tar
  creating B-6
  displaying the contents of B-6
  extracting B-7
  image file format B-25

file system
  displaying available file systems B-2
  displaying file information B-3
  local file system names B-1
  network file system names B-4
  setting the default B-3

filtering
  in a VLAN 33-29
  IPv6 traffic 40-3, 40-7
  non-IP traffic 33-27
  show and more command output 2-10

filtering show and more command output 2-10

filters, IP
  See ACLs, IP

flash device, number of B-1

flexible authentication ordering
  configuring 9-66
  overview 9-31

Flex Link Multicast Fast Convergence 19-3

Flex Links
  configuration guidelines 19-8
  configuring 19-9, 19-10
  configuring preferred VLAN 19-12
  configuring VLAN load balancing 19-11
  default configuration 19-8
  description 19-1
  link load balancing 19-3
  monitoring 19-14
  VLANs 19-3

flooding traffic, blocking 23-8

flow-based packet classification 1-12

flowcharts
  QoS classification 34-7
  QoS egress queueing and scheduling 34-18
  QoS ingress queueing and scheduling 34-16
  QoS policing and marking 34-11

flowcontrol
  configuring 11-20
  described 11-20

forward-delay time
  MSTP 17-24
  STP 26-21

Forwarding Information Base
  See FIB

forwarding nonroutable protocols 47-1

FTP
  accessing MIB files A-4
  configuration files
    downloading B-13
    overview B-12
    preparing the server B-13
    uploading B-15
  image files
    deleting old image B-32
    downloading B-31
    preparing the server B-30
    uploading B-33

G

general query 19-5

Generating IGMP Reports 19-4

get-bulk-request operation 31-3

get-next-request operation 31-3, 31-4

get-request operation 31-3, 31-4

get-response operation 31-3

global configuration mode 2-2

global leave, IGMP 22-13

guest VLAN and 802.1x 9-23

guide mode 1-2
GUIs

See device manager and Network Assistant

H

hardware limitations and Layer 3 interfaces 11-26

hello time

MSTP 17-24

STP 26-20

help, for the command line 2-3

HFTM space 48-24

hierarchical policy maps 34-9

configuration guidelines 34-38

configuring 34-57

described 34-12

history

changing the buffer size 2-6

described 2-6

disabling 2-7

recalling commands 2-6

history table, level and number of syslog messages 30-10

host names, in clusters 5-14

host ports

configuring 15-11

kinds of 15-2

hosts, limit on dynamic ports 13-33

Hot Standby Router Protocol

See HSRP

HP OpenView 1-5

HQATM space 48-24

HSRP

authentication string 41-10

automatic cluster recovery 5-13

binding to cluster group 41-12

cluster standby group considerations 5-12

command-switch redundancy 1-1, 1-7

configuring 41-4

default configuration 41-5

definition 41-1

HSRP (continued)

guidelines 41-6

monitoring 41-13

object tracking 43-7

overview 41-1

priority 41-8

routing redundancy 1-13

support for ICMP redirect messages 41-12

timers 41-10

tracking 41-8

See also clusters, cluster standby group, and standby command switch

HSRP for IPv6

configuring 38-24

guidelines 38-23

HTTP over SSL

see HTTPS

HTTPS 8-50

configuring 8-54

self-signed certificate 8-50

HTTP secure server 8-50

Hulc Forwarding TCAM Manager

See HFTM space

Hulc QoS/ACL TCAM Manager

See HQATM space

IBPG 37-41

ICMP

IPv6 38-4

redirect messages 37-11

support for 1-14

time-exceeded messages 48-16

traceroute and 48-16

unreachable messages 33-20

unreachable messages and IPv6 40-4

unreachables and ACLs 33-21
ICMP Echo operation
  configuring  42-12
IP SLAs  42-12

ICMP ping
  executing  48-13
  overview  48-13

ICMP Router Discovery Protocol
  See IRDP
ICMPv6  38-4

IDS appliances
  and ingress RSPAN  28-21
  and ingress SPAN  28-14

IEEE 802.1D
  See STP
IEEE 802.1p  12-1
IEEE 802.1Q
  and trunk ports  11-3
  configuration limitations  13-18
  encapsulation  13-16
  native VLAN for untagged traffic  13-24
  tunneling
    compatibility with other features  16-6
    defaults  16-4
    described  16-1
  tunnel ports with other features  16-6

IEEE 802.1s
  See MSTP
IEEE 802.1w
  See RSTP
IEEE 802.1x
  See port-based authentication

IEEE 802.3ad
  See EtherChannel
IEEE 802.3af
  See PoE
IEEE 802.3x flow control  11-20

IGMP
  configurable leave timer
    described  22-6
    enabling  22-11
  configuring the switch
    as a member of a group  45-39
    statically connected member  45-43
  controlling access to groups  45-40
  default configuration  45-39
  deleting cache entries  45-62
  displaying groups  45-62
  fast switching  45-44
  flooded multicast traffic
    controlling the length of time  22-12
    disabling on an interface  22-13
    global leave  22-13
    query solicitation  22-13
    recovering from flood mode  22-13
  host-query interval, modifying  45-41
  joining multicast group  22-3
  join messages  22-3
  leave processing, enabling  22-11, 39-9
  leaving multicast group  22-5
  multicast reachability  45-39
  overview  45-3
  queries  22-4
  report suppression
    described  22-6
    disabling  22-16, 39-11
  supported versions  22-3
  support for  1-4
  Version 1
    changing to Version 2  45-41
    described  45-3

ifIndex values, SNMP  31-5
IFS  1-6
IGMP (continued)

Version 2
  changing to Version 1 45-41
  described 45-3
  maximum query response time value 45-43
  pruning groups 45-43
  query timeout value 45-42

IGMP filtering
  configuring 22-26
  default configuration 22-26
  described 22-25
  monitoring 22-30
  support for 1-4

IGMP groups
  configuring filtering 22-29
  setting the maximum number 22-28

IGMP helper 1-4, 45-6

IGMP Immediate Leave
  configuration guidelines 22-11
  described 22-6
  enabling 22-11

IGMP profile
  applying 22-27
  configuration mode 22-26
  configuring 22-27

IGMP snooping
  and address aliasing 22-2
  configuring 22-7
  default configuration 22-7, 39-6
  definition 22-2
  enabling and disabling 22-7, 39-7
  global configuration 22-7
  Immediate Leave 22-6
  method 22-8
  monitoring 22-16, 39-12
  querier
    configuration guidelines 22-14
    configuring 22-14
    supported versions 22-3

IGMP snooping (continued)
  support for 1-4
  VLAN configuration 22-8

IGMP throttling
  configuring 22-29
  default configuration 22-26
  described 22-25
  displaying action 22-30

IGP 37-24
Immediate Leave, IGMP 22-6
  enabling 39-9
  inaccessible authentication bypass 9-25
  support for multiauth ports 9-25
initial configuration
  defaults 1-16
  Express Setup 1-2
interface
  number 11-11
  range macros 11-13
  interface command 11-11
  interface configuration mode 2-3
interfaces
  auto-MDIX, configuring 11-21
  configuration guidelines
    duplex and speed 11-18
  configuring
    procedure 11-11
  counters, clearing 11-32
  default configuration 11-15
  described 11-25
  descriptive name, adding 11-25
  displaying information about 11-31
  flow control 11-20
  management 1-5
  monitoring 11-31
  naming 11-25
  physical, identifying 11-11
  range of 11-12
  restarting 11-33
interfaces (continued)
  shutting down 11-33
  speed and duplex, configuring 11-19
  status 11-31
  supported 11-11
  types of 11-1
interfaces range macro command 11-13
interface types 11-11
Interior Gateway Protocol
  See IGP
internal BGP
  See IBGP
internal neighbors, BGP 37-46
Internet Control Message Protocol
  See ICMP
Internet Group Management Protocol
  See IGMP
Internet Protocol version 6
  See IPv6
Inter-Switch Link
  See ISL
inter-VLAN routing 1-13, 37-2
Intrusion Detection System
  See IDS appliances
inventory management TLV 25-3, 25-8
IP ACLs
  for QoS classification 34-8
  implicit deny 33-9, 33-13
  implicit masks 33-9
  named 33-14
  undefined 33-20
IP addresses
  128-bit 38-2
  candidate or member 5-3, 5-14
  classes of 37-5
  cluster access 5-2
  command switch 5-3, 5-12, 5-14
  default configuration 37-4
  discovering 6-30
IP addresses (continued)
  for IP routing 37-4
  IPv6 38-2
  MAC address association 37-8
  monitoring 37-17
  redundant clusters 5-12
  standby command switch 5-12, 5-14
  See also IP information
IP base image 1-1
IP broadcast address 37-15
ip cef distributed command 37-88
IP directed broadcasts 37-13
ip igmp profile command 22-26
IP information
  assigned
    manually 3-15
  through DHCP-based autoconfiguration 3-3
  default configuration 3-3
IP multicast routing
  addresses
    all-hosts 45-3
    all-multicast-routers 45-3
    host group address range 45-3
    administratively-scoped boundaries, described 45-47
    and IGMP snooping 22-2
    Auto-RP
      adding to an existing sparse-mode cloud 45-26
      benefits of 45-26
      clearing the cache 45-62
      configuration guidelines 45-11
      filtering incoming RP announcement messages 45-29
      overview 45-6
      preventing candidate RP spoofing 45-29
      preventing join messages to false RPs 45-28
      setting up in a new internetwork 45-26
      using with BSR 45-34
IP multicasting routing (continued)

- Bootstrap router
  - Configuration guidelines 45-11
  - Configuring candidate BSRs 45-32
  - Configuring candidate RPs 45-33
  - Defining the IP multicast boundary 45-31
  - Defining the PIM domain border 45-30
  - Overview 45-7
  - Using with Auto-RP 45-34

Cisco implementation 45-2

Configuring
- Basic multicast routing 45-12
- IP multicast boundary 45-47

Default configuration 45-10

Enabling
- Multicast forwarding 45-12
- PIM mode 45-13

Group-to-RP mappings
- Auto-RP 45-6
- BSR 45-7

MBONE
- Deleting sdr cache entries 45-62
- Described 45-45
- Displaying sdr cache 45-63
- Enabling sdr listener support 45-46
- Limiting DVMRP routes advertised 45-57
- Limiting sdr cache entry lifetime 45-46
- SAP packets for conference session announcement 45-46
- Session Directory (sdr) tool, described 45-45

Monitoring
- Packet rate loss 45-63
- Peering devices 45-63
- Tracing a path 45-63

Multicast forwarding, described 45-8

PIMv1 and PIMv2 interoperability 45-11

Protocol interaction 45-2

Reverse path check (RPF) 45-8

IP multicasting routing (continued)

Routing table
- Deleting 45-62
- Displaying 45-63

RP
- Assigning manually 45-24
- Configuring Auto-RP 45-26
- Configuring PIMv2 BSR 45-30
- Monitoring mapping information 45-34
- Using Auto-RP and BSR 45-34

Statistics, displaying system and network 45-62

See also CGMP
See also DVMRP
See also IGMP
See also PIM

IP phones
- And QoS 12-1
  - Automatic classification and queueing 34-21
    - Configuring 12-5
  - Ensuring port security with QoS 34-43
  - Trusted boundary for QoS 34-43

IP Port Security for Static Hosts
- On a Layer 2 access port 20-21
- On a PVLAN host port 20-24

IP precedence 34-2

IP-precedence-to-DSCP map for QoS 34-68

IP protocols
- In ACLs 33-11
  - Routing 1-13

IP routes, monitoring 37-104

IP routing
- Connecting interfaces with 11-10
  - Disabling 37-18
  - Enabling 37-18

IP Service Level Agreements
  - See IP SLAs

IP service levels, analyzing 42-1

IP services image 1-1
IP SLAs

benefits 42-2
configuration guidelines 42-6
configuring object tracking 43-9
Control Protocol 42-4
default configuration 42-6
definition 42-1
ICMP echo operation 42-12
measuring network performance 42-3
monitoring 42-14
multioperations scheduling 42-5
object tracking 43-9
operation 42-3
reachability tracking 43-9
responder
  described 42-4
  enabling 42-8
response time 42-4
scheduling 42-5
SNMP support 42-2
supported metrics 42-2
threshold monitoring 42-6
track object monitoring agent, configuring 43-11
track state 43-9
UDP jitter operation 42-9

IP source guard (continued)
configuration guidelines 20-19
default configuration 20-19
described 20-17
disabling 20-20
displaying
  active IP or MAC bindings 20-26
  bindings 20-26
  configuration 20-26
enabling 20-20, 20-21
filtering
  source IP address 20-17
  source IP and MAC address 20-17
  source IP address filtering 20-17
  source IP and MAC address filtering 20-17
static bindings
  adding 20-20, 20-21
  deleting 20-20
  static hosts 20-21
IP traceroute
  executing 48-17
  overview 48-16
IP unicast routing
  address resolution 37-8
  administrative distances 37-90, 37-101
ARP 37-8
  assigning IP addresses to Layer 3 interfaces 37-5
  authentication keys 37-102
  broadcast
    address 37-15
    flooding 37-16
    packets 37-13
    storms 37-13
  classless routing 37-6
  configuring static routes 37-89

IP source guard
and 802.1x 20-19
and DHCP snooping 20-17
and EtherChannels 20-19
and port security 20-19
and private VLANs 20-19
and routed ports 20-19
and TCAM entries 20-19
and trunk interfaces 20-19
and VRF 20-19
binding configuration
  automatic 20-17
  manual 20-17
binding table 20-17
IP unicast routing (continued)

default
  addressing configuration 37-4
gateways 37-11
networks 37-91
routes 37-91
routing 37-2
directed broadcasts 37-13
disabling 37-18
dynamic routing 37-3
enabling 37-18
EtherChannel Layer 3 interface 37-3
IGP 37-24
inter-VLAN 37-2
IP addressing
  classes 37-5
  configuring 37-4
IPv6 38-3
IRDP 37-11
Layer 3 interfaces 37-3
MAC address and IP address 37-8
passive interfaces 37-100
protocols
  distance-vector 37-3
dynamic 37-3
  link-state 37-3
proxy ARP 37-8
redistribution 37-91
reverse address resolution 37-8
routed ports 37-3
static routing 37-3
steps to configure 37-4
subnet mask 37-5
subnet zero 37-6
supernet 37-6
UDP 37-14
with SVIs 37-3
See also BGP
See also EIGRP

IP unicast routing (continued)

See also OSPF
See also RIP
IPv4 ACLs
  applying to interfaces 33-19
  extended, creating 33-10
  named 33-14
  standard, creating 33-9
IPv4 and IPv6
dual protocol stacks 38-5
IPv6
  ACLs
    displaying 40-8
    limitations 40-3
    matching criteria 40-3
    port 40-1
    precedence 40-2
    router 40-1
    supported 40-2
addresses 38-2
address formats 38-2
applications 38-5
assigning address 38-11
autoconfiguration 38-5
CEFv6 38-18
configuring static routes 38-19
default configuration 38-10
default router preference (DRP) 38-5
defined 38-2
Enhanced Interior Gateway Routing Protocol (EIGRP)
IPv6 38-7
  EIGRP IPv6 Commands 38-7
  Router ID 38-7
feature limitations 38-9
features not supported 38-8
forwarding 38-11
ICMP 38-4
monitoring 38-26
neighbor discovery 38-4
IPv6 (continued)
  OSPF  38-7
  path MTU discovery  38-4
  SDM templates  7-2, 39-1, 40-1
  Stateless Autoconfiguration  38-5
  supported features  38-3
  switch limitations  38-9
  understanding static routes  38-6
IPv6 traffic, filtering  40-3
IRDP
  configuring  37-12
  definition  37-11
  support for  1-14
IS-IS
  addresses  37-63
  area routing  37-63
  default configuration  37-64
  monitoring  37-72
  show commands  37-72
  system routing  37-63
ISL
  and IPv6  38-3
  and trunk ports  11-3
  encapsulation  1-8, 13-16
  trunking with IEEE 802.1 tunneling  16-5
ISO CLNS
  clear commands  37-72
  dynamic routing protocols  37-62
  monitoring  37-72
  NETs  37-62
  NSAPs  37-62
  OSI standard  37-62
ISO IGRP
  area routing  37-63
  system routing  37-63
isolated port  15-2
isolated VLANs  15-2, 15-3

J

join messages, IGMP  22-3

K

KDC
  described  8-40
  See also Kerberos
Kerberos
  authenticating to
    boundary switch  8-42
    KDC  8-42
    network services  8-43
  configuration examples  8-39
  configuring  8-43
  credentials  8-40
  cryptographic software image  8-39
  described  8-40
  KDC  8-40
  operation  8-42
  realm  8-41
  server  8-41
  support for  1-11
  switch as trusted third party  8-40
  terms  8-40
  TGT  8-41
  tickets  8-40
key distribution center
  See KDC

L

l2protocol-tunnel command  16-13
LACP
  Layer 2 protocol tunneling  16-9
  See EtherChannel
Layer 2 frames, classification with CoS  34-2
Layer 2 interfaces, default configuration  11-15
Layer 2 protocol tunneling
  configuring  16-10
  configuring for EtherChannels  16-14
  default configuration  16-11
  defined  16-8
  guidelines  16-11
Layer 2 traceroute
  and ARP  48-15
  and CDP  48-15
  broadcast traffic  48-15
  described  48-15
  IP addresses and subnets  48-15
  MAC addresses and VLANs  48-15
  multicast traffic  48-15
  multiple devices on a port  48-16
  unicast traffic  48-15
  usage guidelines  48-15
Layer 3 features  1-13
Layer 3 interfaces
  assigning IP addresses to  37-5
  assigning IPv4 and IPv6 addresses to  38-14
  assigning IPv6 addresses to  38-11
  changing from Layer 2 mode  37-5, 37-80
  types of  37-3
Layer 3 packets, classification methods  34-2
LDAP  4-2
Leaking IGMP Reports  19-4
LEDs, switch
  See hardware installation guide
lightweight directory access protocol
  See LDAP
line configuration mode  2-3
Link Aggregation Control Protocol
  See EtherChannel
link failure, detecting unidirectional  17-8
Link Layer Discovery Protocol
  See CDP
link local unicast addresses  38-4
link redundancy
  See Flex Links
links, unidirectional  27-1
link state advertisements (LSAs)  37-29
link-state protocols  37-3
link-state tracking
  configuring  35-23
  described  35-21
LLDP
  configuring  25-5
  characteristics  25-7
  default configuration  25-5
  enabling  25-6
  monitoring and maintaining  25-12
  overview  25-1
  supported TLVs  25-2
  switch stack considerations  25-2
  transmission timer and holdtime, setting  25-7
LLDP-MED
  configuring
    procedures  25-5
    TLVs  25-8
  monitoring and maintaining  25-12
  overview  25-1, 25-2
  supported TLVs  25-2
LLDP Media Endpoint Discovery
  See LLDP-MED
load balancing  41-4
local SPAN  28-2
location TLV  25-3, 25-8
logging messages, ACL  33-8
login authentication
  with RADIUS  8-29
  with TACACS+  8-14
login banners  6-17
log messages
  See system message logging
Long-Reach Ethernet (LRE) technology  1-20
<table>
<thead>
<tr>
<th>Term</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>LRE profiles, considerations in switch clusters</td>
<td>5-15</td>
</tr>
<tr>
<td>MAC address-table move update</td>
<td>19-8</td>
</tr>
<tr>
<td>configuration guidelines</td>
<td>19-8</td>
</tr>
<tr>
<td>configuring</td>
<td>19-12</td>
</tr>
<tr>
<td>default configuration</td>
<td>19-8</td>
</tr>
<tr>
<td>description</td>
<td>19-6</td>
</tr>
<tr>
<td>monitoring</td>
<td>19-14</td>
</tr>
<tr>
<td>MAC address-to-VLAN mapping</td>
<td>13-28</td>
</tr>
<tr>
<td>MAC authentication bypass</td>
<td>9-39</td>
</tr>
<tr>
<td>configuring</td>
<td>9-59</td>
</tr>
<tr>
<td>overview</td>
<td>9-17</td>
</tr>
<tr>
<td>MAC extended access lists</td>
<td>33-28</td>
</tr>
<tr>
<td>applying to Layer 2 interfaces</td>
<td>33-28</td>
</tr>
<tr>
<td>configuring for QoS</td>
<td>34-50</td>
</tr>
<tr>
<td>creating</td>
<td>33-27</td>
</tr>
<tr>
<td>defined</td>
<td>33-27</td>
</tr>
<tr>
<td>for QoS classification</td>
<td>34-5</td>
</tr>
<tr>
<td>magic packet</td>
<td>9-28</td>
</tr>
<tr>
<td>manageability features</td>
<td>1-5</td>
</tr>
<tr>
<td>management access</td>
<td>1-5</td>
</tr>
<tr>
<td>in-band</td>
<td>1-5</td>
</tr>
<tr>
<td>browser session</td>
<td>1-6</td>
</tr>
<tr>
<td>CLI session</td>
<td>1-6</td>
</tr>
<tr>
<td>device manager</td>
<td>1-6</td>
</tr>
<tr>
<td>SNMP</td>
<td>1-6</td>
</tr>
<tr>
<td>out-of-band console port connection</td>
<td>1-6</td>
</tr>
<tr>
<td>management address TLV</td>
<td>25-2</td>
</tr>
<tr>
<td>management options</td>
<td>2-1</td>
</tr>
<tr>
<td>CLI</td>
<td>2-1</td>
</tr>
<tr>
<td>clustering</td>
<td>1-3</td>
</tr>
<tr>
<td>CNS</td>
<td>4-1</td>
</tr>
<tr>
<td>Network Assistant</td>
<td>1-2</td>
</tr>
<tr>
<td>overview</td>
<td>1-5</td>
</tr>
<tr>
<td>management VLAN</td>
<td>5-8</td>
</tr>
<tr>
<td>considerations in switch clusters</td>
<td>5-8</td>
</tr>
<tr>
<td>discovery through different management VLANs</td>
<td>5-8</td>
</tr>
<tr>
<td>MAC address learning</td>
<td>1-6</td>
</tr>
<tr>
<td>MAC address learning, disabling on a VLAN</td>
<td>6-29</td>
</tr>
<tr>
<td>MAC address notification, support for</td>
<td>1-15</td>
</tr>
<tr>
<td>MAC addresses</td>
<td>6-21</td>
</tr>
<tr>
<td>aging time</td>
<td>6-21</td>
</tr>
<tr>
<td>and VLAN association</td>
<td>6-20</td>
</tr>
<tr>
<td>building the address table</td>
<td>6-20</td>
</tr>
<tr>
<td>default configuration</td>
<td>6-21</td>
</tr>
<tr>
<td>disabling learning on a VLAN</td>
<td>6-29</td>
</tr>
<tr>
<td>discovering</td>
<td>6-30</td>
</tr>
<tr>
<td>displaying</td>
<td>6-30</td>
</tr>
<tr>
<td>displaying in the IP source binding table</td>
<td>20-26</td>
</tr>
<tr>
<td>dynamic learning</td>
<td>6-20</td>
</tr>
<tr>
<td>removing</td>
<td>6-22</td>
</tr>
<tr>
<td>in ACLs</td>
<td>33-27</td>
</tr>
<tr>
<td>IP address association</td>
<td>37-8</td>
</tr>
<tr>
<td>static adding</td>
<td>6-27</td>
</tr>
<tr>
<td>allowing</td>
<td>6-28, 6-29</td>
</tr>
<tr>
<td>characteristics of</td>
<td>6-26</td>
</tr>
<tr>
<td>dropping</td>
<td>6-28</td>
</tr>
<tr>
<td>removing</td>
<td>6-27</td>
</tr>
<tr>
<td>MAC address learning</td>
<td>1-6</td>
</tr>
<tr>
<td>MAC address-table move update</td>
<td>19-8</td>
</tr>
<tr>
<td>configuration guidelines</td>
<td>19-8</td>
</tr>
<tr>
<td>configuring</td>
<td>19-12</td>
</tr>
<tr>
<td>default configuration</td>
<td>19-8</td>
</tr>
<tr>
<td>description</td>
<td>19-6</td>
</tr>
<tr>
<td>monitoring</td>
<td>19-14</td>
</tr>
<tr>
<td>MAC address-to-VLAN mapping</td>
<td>13-28</td>
</tr>
<tr>
<td>MAC authentication bypass</td>
<td>9-39</td>
</tr>
<tr>
<td>configuring</td>
<td>9-59</td>
</tr>
<tr>
<td>overview</td>
<td>9-17</td>
</tr>
<tr>
<td>MAC extended access lists</td>
<td>33-28</td>
</tr>
<tr>
<td>applying to Layer 2 interfaces</td>
<td>33-28</td>
</tr>
<tr>
<td>configuring for QoS</td>
<td>34-50</td>
</tr>
<tr>
<td>creating</td>
<td>33-27</td>
</tr>
<tr>
<td>defined</td>
<td>33-27</td>
</tr>
<tr>
<td>for QoS classification</td>
<td>34-5</td>
</tr>
<tr>
<td>magic packet</td>
<td>9-28</td>
</tr>
<tr>
<td>manageability features</td>
<td>1-5</td>
</tr>
<tr>
<td>management access</td>
<td>1-5</td>
</tr>
<tr>
<td>in-band</td>
<td>1-5</td>
</tr>
<tr>
<td>browser session</td>
<td>1-6</td>
</tr>
<tr>
<td>CLI session</td>
<td>1-6</td>
</tr>
<tr>
<td>device manager</td>
<td>1-6</td>
</tr>
<tr>
<td>SNMP</td>
<td>1-6</td>
</tr>
<tr>
<td>out-of-band console port connection</td>
<td>1-6</td>
</tr>
<tr>
<td>management address TLV</td>
<td>25-2</td>
</tr>
<tr>
<td>management options</td>
<td>2-1</td>
</tr>
<tr>
<td>CLI</td>
<td>2-1</td>
</tr>
<tr>
<td>clustering</td>
<td>1-3</td>
</tr>
<tr>
<td>CNS</td>
<td>4-1</td>
</tr>
<tr>
<td>Network Assistant</td>
<td>1-2</td>
</tr>
<tr>
<td>overview</td>
<td>1-5</td>
</tr>
<tr>
<td>management VLAN</td>
<td>5-8</td>
</tr>
<tr>
<td>considerations in switch clusters</td>
<td>5-8</td>
</tr>
<tr>
<td>discovery through different management VLANs</td>
<td>5-8</td>
</tr>
<tr>
<td>MAC address learning</td>
<td>1-6</td>
</tr>
<tr>
<td>MAC address learning, disabling on a VLAN</td>
<td>6-29</td>
</tr>
<tr>
<td>MAC address notification, support for</td>
<td>1-15</td>
</tr>
</tbody>
</table>
mapping tables for QoS
configuring
  CoS-to-DSCP  34-67
  DSCP  34-66
  DSCP-to-CoS  34-70
  DSCP-to-DSCP-mutation  34-71
  IP-precedence-to-DSCP  34-68
  policed-DSCP  34-69
described  34-13
marking
  action with aggregate policers  34-64
described  34-4, 34-9
matching
  IPv6 ACLs  40-3
matching, IPv4 ACLs  33-7
maximum aging time
  MSTP  17-25
  STP  26-21
maximum hop count, MSTP  17-25
maximum number of allowed devices, port-based authentication  9-39
maximum-paths command  37-50, 37-89
MDA
  configuration guidelines  9-13 to 9-14
described  1-10, 9-13
exceptions with authentication process  9-6
membership mode, VLAN port  13-3
member switch
  automatic discovery  5-5
defined  5-2
managing  5-16
passwords  5-14
recovering from lost connectivity  48-11
requirements  5-3
See also candidate switch, cluster standby group, and standby command switch
memory consistency check routines  1-5, 48-24
memory consistency integrity  1-5, 48-24
messages, to users through banners  6-17
metrics, in BGP  37-50
metric translations, between routing protocols  37-96
metro tags  16-2
MHSRP  41-4
MIBs
  accessing files with FTP  A-4
  location of files  A-4
  overview  31-1
  SNMP interaction with  31-4
  supported  A-1
mirroring traffic for analysis  28-1
mismatches, autonegotiation  48-11
module number  11-11
monitoring
  access groups  33-41
  BGP  37-61
  cables for unidirectional links  27-1
  CDP  24-5
  CEF  37-88
  EIGRP  37-41
  fallback bridging  47-10
  features  1-15
  Flex Links  19-14
  HSRP  41-13
  IEEE 802.1Q tunneling  16-18
IGMP
  filters  22-30
  snooping  22-16, 39-12
interfaces  11-31
IP
  address tables  37-17
  multicast routing  45-61
  routes  37-104
IP SLAs operations  42-14
IPv4 ACL configuration  33-41
IPv6  38-26
monitoring (continued)
IPv6 ACL configuration 40-8
IS-IS 37-72
ISO CLNS 37-72
Layer 2 protocol tunneling 16-18
MAC address-table move update 19-14
MSDP peers 46-18
multicast router interfaces 22-17, 39-12
multi-VRF CE 37-87
MVR 22-24
network traffic for analysis with probe 28-2
object tracking 43-13
OSPF 37-33
port
  blocking 23-20
  protection 23-20
private VLANs 15-14
RP mapping information 45-34
SFP status 11-31, 48-13
source-active messages 46-18
speed and duplex mode 11-19
SSM mapping 45-22
traffic flowing among switches 29-2
traffic suppression 23-20
tunneling 16-18
VLAN
  filters 33-41
  maps 33-41
VLANs 13-15
VMPS 13-33
VTP 14-16
mrouter Port 19-3
mrouter port 19-5
MSDP
  benefits of 46-3
  clearing MSDP connections and statistics 46-18
MSDP (continued)
  controlling source information
    forwarded by switch 46-11
    originated by switch 46-8
    received by switch 46-13
  default configuration 46-4
  dense-mode regions
    sending SA messages to 46-16
    specifying the originating address 46-17
  filtering
    incoming SA messages 46-14
    SA messages to a peer 46-12
    SA requests from a peer 46-10
  join latency, defined 46-6
  meshed groups
    configuring 46-15
    defined 46-15
    originating address, changing 46-17
    overview 46-1
    peer-RPF flooding 46-2
    peers
      configuring a default 46-4
      monitoring 46-18
      peering relationship, overview 46-1
      requesting source information from 46-8
      shutting down 46-15
    source-active messages
      caching 46-6
      clearing cache entries 46-18
      defined 46-2
      filtering from a peer 46-10
      filtering incoming 46-14
      filtering to a peer 46-12
      limiting data with TTL 46-13
      monitoring 46-18
      restricting advertised sources 46-9
      support for 1-14
MSTP

boundary ports
configuration guidelines 17-15
described 17-6

BPDU filtering
described 18-3
enabling 18-13

BPDU guard
described 18-2
enabling 18-12

CIST, described 17-3
CIST regional root 17-3
CIST root 17-5
configuration guidelines 17-15, 18-10
configuring
forward-delay time 17-24
hello time 17-24
link type for rapid convergence 17-26
maximum aging time 17-25
maximum hop count 17-25
MST region 17-16
neighbor type 17-26
path cost 17-21
port priority 17-20
root switch 17-18
secondary root switch 17-19
switch priority 17-23

CST
defined 17-3
operations between regions 17-3
default configuration 17-15
default optional feature configuration 18-10
displaying status 17-27
enabling the mode 17-16
EtherChannel guard
described 18-7
enabling 18-15

MSTP (continued)
extended system ID
effects on root switch 17-18
effects on secondary root switch 17-19
unexpected behavior 17-18

IEEE 802.1s
implementation 17-7
port role naming change 17-7
terminology 17-5
instances supported 26-9
interface state, blocking to forwarding 18-2
interoperability and compatibility among modes 26-10
interoperability with IEEE 802.1D
described 17-8
restarting migration process 17-27

IST
defined 17-2
master 17-3
operations within a region 17-3
loop guard
described 18-9
enabling 18-16
mapping VLANs to MST instance 17-16

MST region
CIST 17-3
configuring 17-16
described 17-2
hop-count mechanism 17-6
IST 17-2
supported spanning-tree instances 17-2
optional features supported 1-8
overview 17-2
Port Fast
described 18-2
enabling 18-10
preventing root switch selection 18-8
MSTP (continued)
  root guard
    described 18-8
    enabling 18-16
  root switch
    configuring 17-18
    effects of extended system ID 17-18
    unexpected behavior 17-18
  shutdown Port Fast-enabled port 18-2
  status, displaying 17-27
  multiauth
    support for inaccessible authentication bypass 9-25
  multiauth mode
    See multiple-authentication mode
  multicast groups
    Immediate Leave 22-6
    joining 22-3
    leaving 22-5
    static joins 22-10, 39-8
  multicast packets
    ACLs on 33-40
    blocking 23-8
  multicast router interfaces, monitoring 22-17, 39-12
  multicast router ports, adding 22-9, 39-8
  Multicast Source Discovery Protocol
    See MSDP
  multicast storm 23-2
  multicast storm-control command 23-4
  multicast television application 22-18
  multicast VLAN 22-18
  Multicast VLAN Registration
    See MVR
  multidomain authentication
    See MDA
  multioperations scheduling, IP SLAs 42-5
  multiple authentication 9-14
  multiple authentication mode
    configuring 9-45
  Multiple HSRP
    See MHSRP
  multiple VPN routing/forwarding in customer edge devices
    See multi-VRF CE
  multi-VRF CE
    configuration example 37-83
    configuration guidelines 37-75
    configuring 37-75
    default configuration 37-75
    defined 37-73
    displaying 37-87
    monitoring 37-87
    network components 37-75
    packet-forwarding process 37-74
    support for 1-13
  MVR
    and address aliasing 22-21
    and IGMPv3 22-21
    configuration guidelines 22-20
    configuring interfaces 22-22
    default configuration 22-20
    described 22-18
    example application 22-18
    modes 22-21
    monitoring 22-24
    multicast television application 22-18
    setting global parameters 22-21
    support for 1-4
  N
  NAC
    AAA down policy 1-11
    critical authentication 9-25, 9-56
    IEEE 802.1x authentication using a RADIUS server 9-61
    IEEE 802.1x validation using RADIUS server inaccessible authentication bypass 1-11, 9-56
NAC (continued)
  Layer 2 IEEE 802.1x validation  1-11, 9-31, 9-61
  Layer 2 IP validation  1-11
named IPv4 ACLs  33-14
NameSpace Mapper
  See NSM
native VLAN
  and IEEE 802.1Q tunneling  16-4
  configuring  13-24
  default  13-24
NEAT
  configuring  9-62
  overview  9-32
neighbor discovery, IPv6  38-4
neighbor discovery/recovery, EIGRP  37-34
neighbors, BGP  37-56
Network Admission Control
  NAC
Network Assistant
  benefits  1-2
  described  1-5
  downloading image files  1-2
  guide mode  1-2
  management options  1-2
  upgrading a switch  B-24
  wizards  1-2
network configuration examples
  increasing network performance  1-19
  large network  1-24
  long-distance, high-bandwidth transport  1-26
  providing network services  1-19
  server aggregation and Linux server cluster  1-22
  small to medium-sized network  1-23
network design
  performance  1-19
  services  1-19
Network Edge Access Topology
  See NEAT
network management
  CDP  24-1
  RMON  29-1
  SNMP  31-1
network performance, measuring with IP SLAs  42-3
network policy TLV  25-2, 25-8
Network Time Protocol
  See NTP
  no commands  2-4
  nonhierarchical policy maps
    configuration guidelines  34-38
    described  34-10
  non-IP traffic filtering  33-27
  nontrunking mode  13-17
  normal-range VLANs  13-4
    configuration guidelines  13-6
    configuring  13-4
    defined  13-1
  no switchport command  11-4
  not-so-stubby areas
    See NSSA
  NSAPs, as ISO IGRP addresses  37-63
  NSF Awareness
    IS-IS  37-65
  NSM  4-3
  NSSA, OSPF  37-29
NTP
  associations
    authenticating  6-5
    defined  6-2
    enabling broadcast messages  6-7
    peer  6-6
    server  6-6
  default configuration  6-4
  displaying the configuration  6-11
  overview  6-2
  restricting access
    creating an access group  6-9
    disabling NTP services per interface  6-10
NTP (continued)
source IP address, configuring 6-10
stratum 6-2
support for 1-6
synchronizing devices 6-6
time
services 6-2
synchronizing 6-2

OSPF (continued)
LSA group pacing 37-32
monitoring 37-33
router IDs 37-32
route summarization 37-30
support for 1-13
virtual links 37-30
out-of-profile markdown 1-13

O

object tracking
HSRP 43-7
IP SLAs 43-9
IP SLAs, configuring 43-9
monitoring 43-13
off mode, VTP 14-3
online diagnostics
overview 49-1
running tests 49-3
understanding 49-1
open1x
configuring 9-67
open1x authentication
overview 9-31
Open Shortest Path First
See OSPF
optimizing system resources 7-1
options, management 1-5
OSPF
area parameters, configuring 37-29
configuring 37-27
default configuration
metrics 37-30
route 37-30
settings 37-25
described 37-24
for IPv6 38-7
interface parameters, configuring 37-28

P

packet modification, with QoS 34-20
PAgP
Layer 2 protocol tunneling 16-9
See EtherChannel
parallel paths, in routing tables 37-89
passive interfaces
configuring 37-100
OSPF 37-31
passwords
default configuration 8-3
disabling recovery of 8-5
encrypting 8-4
for security 1-9
in clusters 5-14
overview 8-1
recovery of 48-3
setting
enable 8-3
enable secret 8-4
Telnet 8-6
with usernames 8-7
VTP domain 14-8
path cost
MSTP 17-21
STP 26-18
path MTU discovery 38-4
PBR
- defined 37-96
- enabling 37-98
- fast-switched policy-based routing 37-99
- local policy-based routing 37-99

PC (passive command switch) 5-11
peers, BGP 37-56
percentage thresholds in tracked lists 43-6
performance, network design 1-19
performance features 1-3
persistent self-signed certificate 8-50
per-user ACLs and Filter-Ids 9-9
per-VLAN spanning-tree plus
  See PVST+
PE to CE routing, configuring 37-82
physical ports 11-2

PIM
- default configuration 45-10
- dense mode
  overview 45-4
  rendezvous point (RP), described 45-5
  RPF lookups 45-8
- displaying neighbors 45-63
- enabling a mode 45-13
- overview 45-4
- router-query message interval, modifying 45-37
- shared tree and source tree, overview 45-35
- shortest path tree, delaying the use of sparse mode
  join messages and shared tree 45-5
  overview 45-5
  prune messages 45-5
  RPF lookups 45-9
- stub routing
  configuration guidelines 45-22
  displaying 45-63
  enabling 45-23
  overview 45-5
- support for 1-14

PIM (continued)
- versions
  interoperability 45-11
  troubleshooting interoperability problems 45-35
  v2 improvements 45-4

PIM-DVMRP, as snooping method 22-8
ping
  character output description 48-14
  executing 48-13
  overview 48-13

PoE
- auto mode 11-9
- CDP with power consumption, described 11-7
- CDP with power negotiation, described 11-7
- Cisco intelligent power management 11-7
- configuring 11-22
- devices supported 11-6
- high-power devices operating in low-power mode 11-7
- IEEE power classification levels 11-8
- power budgeting 11-23
- power consumption 11-23
- powered-device detection and initial power allocation 11-7
- power management modes 11-9
- power negotiation extensions to CDP 11-7
- standards supported 11-7
- static mode 11-9
- troubleshooting 48-11
- policed-DSCP map for QoS 34-69

policers
- configuring
  for each matched traffic class 34-53
  for more than one traffic class 34-64
- described 34-4
- displaying 34-84
- number of 34-39
- types of 34-10
policing
    described 34-4
    hierarchical
      See hierarchical policy maps
token-bucket algorithm 34-10

policy-based routing
    See PBR

policy maps for QoS
    characteristics of 34-53
described 34-8
displaying 34-85
    hierarchical 34-9

hierarchical on SVIs
    configuration guidelines 34-38
    configuring 34-57
described 34-12
nonhierarchical on physical ports
    configuration guidelines 34-38
described 34-10

port ACLs
    defined 33-2
types of 33-3

Port Aggregation Protocol
    See EtherChannel

port-based authentication (continued)
    RADIUS server 9-45, 10-13
    RADIUS server parameters on the switch 9-44, 10-11
    restricted VLAN 9-54
    switch-to-client frame-retransmission number 9-49, 9-50
    switch-to-client retransmission time 9-48
    violation modes 9-41 to 9-42
default configuration 9-36, 10-9
described 9-1
device roles 9-3, 10-2
displaying statistics 9-69, 10-17
downloadable ACLs and redirect URLs
    configuring 9-63 to 9-65, ?? to 9-66
    overview 9-20 to 9-22
    EAPOL-start frame 9-6
    EAP-request/identity frame 9-6
    EAP-response/identity frame 9-6
    enabling
      802.1X authentication 10-11
    encapsulation 9-3
    flexible authentication ordering
    configuring 9-66
    overview 9-31
    guest VLAN
    configuration guidelines 9-23, 9-24
    described 9-23
    host mode 9-12
    inaccessible authentication bypass
    configuring 9-56
described 9-25
guidelines 9-38
    initiation and message exchange 9-6
    magic packet 9-28
    maximum number of allowed devices per port 9-39
    method lists 9-42
    multiple authentication 9-14
port-based authentication (continued)

- per-user ACLs
  - AAA authorization 9-42
  - configuration tasks 9-20
  - described 9-19
  - RADIUS server attributes 9-19

- ports
  - authorization state and dot1x port-control command 9-11
  - authorized and unauthorized 9-11
  - voice VLAN 9-26

- port security
  - and voice VLAN 9-27
  - described 9-27
  - interactions 9-27
  - multiple-hosts mode 9-12

- readiness check
  - configuring 9-39
  - described 9-17, 9-39
  - resetting to default values 9-68

- statistics, displaying 9-69

- switch
  - as proxy 9-3, 10-2
  - RADIUS client 9-3

- switch supplicant
  - configuring 9-62
  - overview 9-32

- upgrading from a previous release 34-32

- user distribution
  - guidelines 9-30
  - overview 9-30

- VLAN assignment
  - AAA authorization 9-42
  - characteristics 9-18
  - configuration tasks 9-19
  - described 9-18

- voice aware 802.1x security
  - configuring 9-40
  - described 9-32, 9-40

port-based authentication (continued)

- voice VLAN
  - described 9-26
  - PVID 9-26
  - VVID 9-26
  - wake-on-LAN, described 9-28
  - with ACLs and RADIUS Filter-Id attribute 9-34

- port-based authentication methods, supported 9-8

- port blocking 1-4, 23-8

- port-channel
  - See EtherChannel

- port description TLV 25-2

- Port Fast
  - described 18-2
  - enabling 18-10
  - mode, spanning tree 13-29
  - support for 1-8

- port membership modes, VLAN 13-3

- port priority
  - MSTP 17-20
  - STP 26-17

- ports
  - access 11-3
  - blocking 23-8
  - dual-purpose uplink 11-6
  - dynamic access 13-3
  - IEEE 802.1Q tunnel 13-4
  - protected 23-6
  - routed 11-4
  - secure 23-9
  - static-access 13-3, 13-9
  - switch 11-2
  - trunks 13-3, 13-16
  - VLAN assignments 13-9

- port security
  - aging 23-18
  - and private VLANs 23-19
  - and QoS trusted boundary 34-43
  - configuring 23-13
port security (continued)
  default configuration 23-11
  described 23-9
  displaying 23-20
  enabling 23-19
  on trunk ports 23-15
  sticky learning 23-10
  violations 23-12
  with other features 23-12

port VLAN ID TLV 25-2
power management TLV 25-2, 25-8

Power over Ethernet
  See PoE
preemption, default configuration 19-8
preemption delay, default configuration 19-8
preferential treatment of traffic
  See QoS
prefix lists, BGP 37-54
preventing unauthorized access 8-1
primary interface for object tracking, DHCP, configuring 43-10
primary interface for static routing, configuring 43-10
primary links 19-2
primary VLANs 15-1, 15-3
priority
  HSRP 41-8
    overriding CoS 12-7
    trusting CoS 12-7
private VLAN edge ports
  See protected ports
private VLANs
  across multiple switches 15-4
  and SDM template 15-4
  and SVIs 15-5
  benefits of 15-1
  community ports 15-2
  community VLANs 15-2, 15-3
  configuration guidelines 15-6, 15-7, 15-8
private VLANs (continued)
  configuration tasks 15-6
  configuring 15-9
  default configuration 15-6
  end station access to 15-3
  IP addressing 15-3
  isolated port 15-2
  isolated VLANs 15-2, 15-3
  mapping 15-13
  monitoring 15-14
  ports
    community 15-2
    configuration guidelines 15-8
    configuring host ports 15-11
    configuring promiscuous ports 15-12
    described 15-4
    isolated 15-2
    promiscuous 15-2
    primary VLANs 15-1, 15-3
    promiscuous ports 15-2
    secondary VLANs 15-2
    subdomains 15-1
    traffic in 15-5
privileged EXEC mode 2-2
privilege levels
  changing the default for lines 8-9
  command switch 5-16
  exiting 8-10
  logging into 8-10
  mapping on member switches 5-16
  overview 8-2, 8-8
  setting a command with 8-8
promiscuous ports
  configuring 15-12
  defined 15-2
protected ports 1-9, 23-6
protocol-dependent modules, EIGRP 37-34
Protocol-Independent Multicast Protocol
  See PIM
provider edge devices 37-73

proxy ARP
  configuring 37-10
  definition 37-8
  with IP routing disabled 37-11

proxy reports 19-4

pruning, VTP
  disabling
    in VTP domain 14-14
    on a port 13-23
  enabling
    in VTP domain 14-14
    on a port 13-23
  examples 14-6
  overview 14-5

pruning-eligible list
  changing 13-23
  for VTP pruning 14-5
  VLANs 14-14

PVST+
  described 26-9
  IEEE 802.1Q trunking interoperability 26-10
  instances supported 26-9

QoS (continued)

classification
  class maps, described 34-8
  defined 34-4
  DSCP transparency, described 34-45
  flowchart 34-7
  forwarding treatment 34-3
  in frames and packets 34-3
  IP ACLs, described 34-6, 34-8
  MAC ACLs, described 34-5, 34-8
  options for IP traffic 34-6
  options for non-IP traffic 34-5
  policy maps, described 34-8
  trust DSCP, described 34-5
  trusted CoS, described 34-5
  trust IP precedence, described 34-5

class maps
  configuring 34-51
  displaying 34-84

configuration guidelines
  auto-QoS 34-31
  standard QoS 34-37

configuring
  aggregate policers 34-64
  auto-QoS 34-21
  default port CoS value 34-43
  DSCP maps 34-66
  DSCP transparency 34-45
  DSCP trust states bordering another domain 34-45
  egress queue characteristics 34-77
  ingress queue characteristics 34-72
  IP extended ACLs 34-49
  IP standard ACLs 34-48
  MAC ACLs 34-50
  policy maps, hierarchical 34-57
  port trust states within the domain 34-41
  trusted boundary 34-43
  default auto configuration 34-21

QoS

and MQC commands 34-1

auto-QoS
  categorizing traffic 34-21
  configuration and defaults display 34-34
  configuration guidelines 34-31
  described 34-21
  disabling 34-34
  displaying generated commands 34-34
  displaying the initial configuration 34-34
  effects on running configuration 34-31
  list of generated commands 34-24
  basic model 34-4
QoS (continued)

default standard configuration 34-35
displaying statistics 34-84
DSCP transparency 34-45
egress queues
allocating buffer space 34-78
buffer allocation scheme, described 34-18
configuring shaped weights for SRR 34-81
configuring shared weights for SRR 34-82
described 34-4
displaying the threshold map 34-80
flowchart 34-18
mapping DSCP or CoS values 34-80
scheduling, described 34-4
setting WTD thresholds 34-78
WTD, described 34-19
enabling globally 34-40
flowcharts
classification 34-7
egress queueing and scheduling 34-18
ingress queueing and scheduling 34-16
policing and marking 34-11
implicit deny 34-8
ingress queues
allocating bandwidth 34-75
allocating buffer space 34-74
buffer and bandwidth allocation, described 34-17
configuring shared weights for SRR 34-75
configuring the priority queue 34-76
described 34-4
displaying the threshold map 34-74
flowchart 34-16
mapping DSCP or CoS values 34-73
priority queue, described 34-17
scheduling, described 34-4
setting WTD thresholds 34-73
WTD, described 34-17
QoS (continued)

IP phones
automatic classification and queueing 34-21
detection and trusted settings 34-21, 34-43
limiting bandwidth on egress interface 34-83
mapping tables
CoS-to-DSCP 34-67
displaying 34-84
DSCP-to-CoS 34-70
DSCP-to-DSCP-mutation 34-71
IP-precedence-to-DSCP 34-68
policing-DSCP 34-69
types of 34-13
marked-down actions 34-55, 34-61
marking, described 34-4, 34-9
overview 34-2
packet modification 34-20
policers
configuring 34-55, 34-61, 34-65
described 34-9
displaying 34-84
number of 34-39
types of 34-10
policies, attaching to an interface 34-9
policing
described 34-4, 34-9
token bucket algorithm 34-10
policy maps
characteristics of 34-53
displaying 34-85
hierarchical 34-9
hierarchical on SVIs 34-57
nonhierarchical on physical ports 34-53
QoS label, defined 34-4

IP phones
automatic classification and queueing 34-21
detection and trusted settings 34-21, 34-43
limiting bandwidth on egress interface 34-83
mapping tables
CoS-to-DSCP 34-67
displaying 34-84
DSCP-to-CoS 34-70
DSCP-to-DSCP-mutation 34-71
IP-precedence-to-DSCP 34-68
policing-DSCP 34-69
types of 34-13
marked-down actions 34-55, 34-61
marking, described 34-4, 34-9
overview 34-2
packet modification 34-20
policers
configuring 34-55, 34-61, 34-65
described 34-9
displaying 34-84
number of 34-39
types of 34-10
policies, attaching to an interface 34-9
policing
described 34-4, 34-9
token bucket algorithm 34-10
policy maps
characteristics of 34-53
displaying 34-85
hierarchical 34-9
hierarchical on SVIs 34-57
nonhierarchical on physical ports 34-53
QoS label, defined 34-4
QoS (continued)

queues
   configuring egress characteristics  34-77
   configuring ingress characteristics  34-72
   high priority (expedite)  34-20, 34-83
   location of  34-14
   SRR, described  34-15
   WTD, described  34-14
rewrites  34-20
support for  1-12
trust states
   bordering another domain  34-45
   described  34-5
   trusted device  34-43
   within the domain  34-41
quality of service
   See QoS
queries, IGMP  22-4
query solicitation, IGMP  22-13

R

RADIUS (continued)

   method list, defined  8-26
   operation of  8-20
   overview  8-18
   server load balancing  8-39
   suggested network environments  8-19
   support for  1-11
   tracking services accessed by user  8-34
RADIUS Change of Authorization  8-20
range
   macro  11-13
   of interfaces  11-12
   rapid convergence  17-10
   rapid per-VLAN spanning-tree plus
      See rapid PVST+
   rapid PVST+
      described  26-9
      IEEE 802.1Q trunking interoperability  26-10
      instances supported  26-9
Rapid Spanning Tree Protocol
   See RSTP
RARP  37-8
rcommand command  5-16
RCP
   configuration files
      downloading  B-17
      overview  B-16
      preparing the server  B-16
      uploading  B-18
   image files
      deleting old image  B-37
      downloading  B-35
      preparing the server  B-34
      uploading  B-37
   reachability, tracking IP SLAs IP host  43-9
   readiness check
      port-based authentication
         configuring  9-39
         described  9-17, 9-39
reconfirmation interval, VMPS, changing 13-32
reconfirming dynamic VLAN membership 13-31
recovery procedures 48-1
redirect URL 9-20, 9-21, 9-63
redundancy
  EtherChannel 35-3
  HSRP 41-1
  STP
    backbone 26-8
    path cost 13-26
    port priority 13-25
redundant links and UplinkFast 18-14
redundant power system
  See Cisco Redundant Power System 2300
reliable transport protocol, EIGRP 37-34
reloading software 3-23
Remote Authentication Dial-In User Service
  See RADIUS
Remote Copy Protocol
  See RCP
Remote Network Monitoring
  See RMON
Remote SPAN
  See RSPAN
remote SPAN 28-2
report suppression, IGMP
  described 22-6
  disabling 22-16, 39-11
resequencing ACL entries 33-14
reserved addresses in DHCP pools 20-28
resets, in BGP 37-49
resetting a UDLD-shutdown interface 27-6
responder, IP SLAs
  described 42-4
  enabling 42-8
response time, measuring with IP SLAs 42-4
restricted VLAN
  configuring 9-54
  described 9-24
  using with IEEE 802.1x 9-24
restricting access
  NTP services 6-8
  overview 8-1
  passwords and privilege levels 8-2
  RADIUS 8-18
  TACACS+ 8-10
retry count, VMPS, changing 13-32
reverse address resolution 37-8
Reverse Address Resolution Protocol
  See RARP
RFC
  1058, RIP 37-18
  1112, IP multicast and IGMP 22-2
  1157, SNMPv1 31-2
  1163, BGP 37-41
  1166, IP addresses 37-5
  1253, OSPF 37-24
  1267, BGP 37-41
  1305, NTP 6-2
  1587, NSSAs 37-24
  1757, RMON 29-2
  1771, BGP 37-41
  1901, SNMPv2c 31-2
  1902 to 1907, SNMPv2 31-2
  2236, IP multicast and IGMP 22-2
  2273-2275, SNMPv3 31-2
RFC 5176 Compliance 8-21
RIP
  advertisements 37-19
  authentication 37-21
  configuring 37-20
  default configuration 37-19
  described 37-19
  for IPv6 38-7
  hop counts 37-19
RIP (continued)
  split horizon 37-22
  summary addresses 37-22
  support for 1-13

RMON
  default configuration 29-3
  displaying status 29-7
  enabling alarms and events 29-3
  groups supported 29-2
  overview 29-2
  statistics
    collecting group Ethernet 29-6
    collecting group history 29-5
  support for 1-15

root guard
  described 18-8
  enabling 18-16
  support for 1-8

root switch
  MSTP 17-18
  STP 26-14

route calculation timers, OSPF 37-31

route dampening, BGP 37-60

routed packets, ACLs on 33-39

routed ports
  configuring 37-3
  defined 11-4
  in switch clusters 5-9
  IP addresses on 11-26, 37-4
  route-map command 37-99

route maps
  BGP 37-52
  policy-based routing 37-96

router ACLs
  defined 33-2
  types of 33-4

route reflectors, BGP 37-59

router ID, OSPF 37-32

route selection, BGP 37-50

route summarization, OSPF 37-30

route targets, VPN 37-75

routing
  default 37-2
  dynamic 37-3
  redistribution of information 37-91
  static 37-3
  routing domain confederation, BGP 37-59

Routing Information Protocol
  See RIP

routing protocol administrative distances 37-90

RPS
  See Cisco Redundant Power System 2300

RPS 2300
  See Cisco Redundant Power System 2300

RSPAN
  characteristics 28-8
  configuration guidelines 28-16
  default configuration 28-10
  defined 28-2
  destination ports 28-7
  displaying status 28-23
  interaction with other features 28-8
  monitored ports 28-5
  monitoring ports 28-7
  overview 1-15, 28-1
  received traffic 28-4
  sessions
    creating 28-17
    defined 28-3
    limiting source traffic to specific VLANs 28-22
    specifying monitored ports 28-17
    with ingress traffic enabled 28-21
    source ports 28-5
    transmitted traffic 28-5
    VLAN-based 28-6
RSTP
  active topology 17-9
  BPDU
    format 17-12
    processing 17-13
designated port, defined 17-9
designated switch, defined 17-9
interoperability with IEEE 802.1D
described 17-8
  restarting migration process 17-27
topology changes 17-13
overview 17-9
port roles
described 17-9
  synchronized 17-11
  proposal-agreement handshake process 17-10
rapid convergence
described 17-10
  edge ports and Port Fast 17-10
  point-to-point links 17-10, 17-26
  root ports 17-10
root port, defined 17-9
See also MSTP
running configuration
replacing B-19, B-20
  rolling back B-19, B-21
running configuration, saving 3-16

SDM
  templates
    configuring 7-4
    number of 7-1
  SDM template 40-3
    configuration guidelines 7-3
    configuring 7-3
    dual IPv4 and IPv6 7-2
    types of 7-1
  secondary VLANs 15-2
  Secure Copy Protocol
  secure HTTP client
    configuring 8-55
    displaying 8-56
  secure HTTP server
    configuring 8-54
    displaying 8-56
  secure MAC addresses
deleing 23-17
  maximum number of 23-10
  types of 23-10
secure ports, configuring 23-9
secure remote connections 8-45
Secure Shell
  See SSH
  Secure Socket Layer
    See SSL
security, port 23-9
  security features 1-9
  See SCP
sequence numbers in log messages 30-8
server mode, VTP 14-3
service-provider network, MSTP and RSTP 17-1
service-provider networks
  and customer VLANs 16-2
  and IEEE 802.1Q tunneling 16-1
  Layer 2 protocols across 16-8
  Layer 2 protocol tunneling for EtherChannels 16-9
set-request operation 31-4
setup program
  failed command switch replacement 48-9
  replacing failed command switch 48-8
severity levels, defining in system messages 30-8
SFPs
  monitoring status of 11-31, 48-13
  security and identification 48-12
  status, displaying 48-13
shaped round robin
  See SRR
show access-lists hw-summary command 33-21
show and more command output, filtering 2-10
show cdp traffic command 24-5
show cluster members command 5-16
show configuration command 11-25
show forward command 48-20
show interfaces command 11-19, 11-25
show interfaces switchport 19-4
show l2protocol command 16-13, 16-15, 16-16
show lldp traffic command 25-12
show platform forward command 48-20
show platform team command 48-24
show running-config command
  displaying ACLs 33-19, 33-20, 33-31, 33-34
  interface description in 11-25
shutdown command on interfaces 11-33
shutdown threshold for Layer 2 protocol packets 16-11
Simple Network Management Protocol
  See SNMP
small-frame arrival rate, configuring 23-5
SNAP 24-1
SNMP
  accessing MIB variables with
    agent described 31-4
    disabling 31-7
    and IP SLAs 42-2
    authentication level 31-10
SNMP (continued)
  community strings
    configuring 31-8
    for cluster switches 31-4
    overview 31-4
  configuration examples 31-17
  default configuration 31-6
  engine ID 31-7
  groups 31-7, 31-9
  host 31-7
  ifIndex values 31-5
  in-band management 1-6
  in clusters 5-15
  informs
    and trap keyword 31-12
    described 31-5
    differences from traps 31-5
    disabling 31-15
    enabling 31-15
  limiting access by TFTP servers 31-16
  limiting system log messages to NMS 30-10
  manager functions 1-5, 31-3
  managing clusters with 5-16
  MIBs
    location of A-4
    supported A-1
    notifications 31-5
    overview 31-1, 31-4
    security levels 31-2
    setting CPU threshold notification 31-15
    status, displaying 31-18
    system contact and location 31-16
    trap manager, configuring 31-13
    traps
      described 31-3, 31-5
      differences from informs 31-5
      disabling 31-15
      enabling 31-12
SNMP (continued)

enabling MAC address notification 6-22, 6-24, 6-25
overview 31-1, 31-4
types of 31-12
users 31-7, 31-9
versions supported 31-2
SNMP and Syslog Over IPv6 38-7
SNMPv1 31-2
SNMPv2C 31-2
SNMPv3 31-2
snooping, IGMP 22-2
software images
location in flash B-25
recovery procedures 48-2
scheduling reloads 3-24
tar file format, described B-25
See also downloading and uploading
source addresses
in IPv4 ACLs 33-11
in IPv6 ACLs 40-5
source-and-destination-IP address based forwarding, EtherChannel 35-8
source-and-destination MAC address forwarding, EtherChannel 35-8
source-IP address based forwarding, EtherChannel 35-8
source-MAC address forwarding, EtherChannel 35-7
Source-specific multicast
See SSM
SPAN (continued)
sessions
configuring ingress forwarding 28-15, 28-22
creating 28-11
defined 28-3
limiting source traffic to specific VLANs 28-15
removing destination (monitoring) ports 28-13
specifying monitored ports 28-11
with ingress traffic enabled 28-14
source ports 28-5
transmitted traffic 28-5
VLAN-based 28-6
spanning tree and native VLANs 13-18
Spanning Tree Protocol
See STP
SPAN traffic 28-4
split horizon, RIP 37-22
SRR
configuring
shaped weights on egress queues 34-81
shared weights on egress queues 34-82
shared weights on ingress queues 34-75
described 34-15
shaped mode 34-15
shared mode 34-15
support for 1-13
SSH
configuring 8-46
cryptographic software image 8-45
described 1-6, 8-45
encryption methods 8-46
user authentication methods, supported 8-46
SSL
configuration guidelines 8-52
configuring a secure HTTP client 8-55
configuring a secure HTTP server 8-54
cryptographic software image 8-49
described 8-49
monitoring 8-56
SSM
address management restrictions 45-16
CGMP limitations 45-16
components 45-14
configuration guidelines 45-15
configuring 45-13, 45-16
differs from Internet standard multicast 45-14
IGMP snooping 45-16
IGMPv3 45-14
IGMPv3 Host Signalling 45-15
IP address range 45-14
monitoring 45-16
operations 45-15
PIM 45-14
state maintenance limitations 45-16
SSM mapping 45-17
configuration guidelines 45-17
configuring 45-17, 45-19
DNS-based 45-18, 45-20
monitoring 45-22
overview 45-18
restrictions 45-18
static 45-18, 45-20
static traffic forwarding 45-21
stacks, switch
MSTP instances supported 26-9
standby command switch
configuring
considerations 5-12
defined 5-2
priority 5-11
requirements 5-3
virtual IP address 5-12
See also cluster standby group and HSRP
standby group, cluster
See cluster standby group and HSRP
standby ip command 41-6
standby links 19-2
standby router 41-1
standby timers, HSRP 41-10
startup configuration
booting
manually 3-20
specific image 3-21
clearing B-19
configuration file
automatically downloading 3-19
specifying the filename 3-19
default boot configuration 3-19
static access ports
assigning to VLAN 13-9
defined 11-3, 13-3
static addresses
See addresses
static IP routing 1-14
static MAC addressing 1-9
static route primary interface, configuring 43-10
static routes
configuring 37-89
configuring for IPv6 38-19
understanding 38-6
static routing 37-3
static routing support, enhanced object tracking 43-10
static SSM mapping 45-18, 45-20
static traffic forwarding 45-21
static VLAN membership 13-2
statistics
802.1X 10-17
802.1x 9-69
CDP 24-5
interface 11-31
IP multicast routing 45-62
LLDP 25-12
LLDP-MED 25-12
NMSP 25-12
OSPF 37-33
QoS ingress and egress 34-84
RMON group Ethernet 29-6
statistics (continued)
- RMON group history 29-5
- SNMP input and output 31-18
- VTP 14-16

sticky learning 23-10

storm control
- configuring 23-3
- described 23-2
- disabling 23-5
- displaying 23-20
- support for 1-4
- thresholds 23-2

STP
- accelerating root port selection 18-4
- BackboneFast
  - described 18-5
  - disabling 18-15
  - enabling 18-14
- BPDU filtering
  - described 18-3
  - disabling 18-13
  - enabling 18-13
- BPDU guard
  - described 18-2
  - disabling 18-12
  - enabling 18-12
- BPDU message exchange 26-3
- configuration guidelines 18-10, 26-12
- configuring
  - forward-delay time 26-21
  - hello time 26-20
  - maximum aging time 26-21
  - path cost 26-18
  - port priority 26-17
  - root switch 26-14
  - secondary root switch 26-16
  - spanning-tree mode 26-13
  - switch priority 26-19
  - transmit hold-count 26-22

STP (continued)
- counters, clearing 26-22
- default configuration 26-11
- default optional feature configuration 18-10
- designated port, defined 26-3
- designated switch, defined 26-3
- detecting indirect link failures 18-5
- disabling 26-14
- displaying status 26-22
- EtherChannel guard
  - described 18-7
  - disabling 18-15
  - enabling 18-15
- extended system ID
  - effects on root switch 26-14
  - effects on the secondary root switch 26-16
  - overview 26-4
  - unexpected behavior 26-15
- features supported 1-7
- IEEE 802.1D and bridge ID 26-4
- IEEE 802.1D and multicast addresses 26-8
- IEEE 802.1t and VLAN identifier 26-4
- inferior BPDU 26-3
- instances supported 26-9
- interface state, blocking to forwarding 18-2
- interface states
  - blocking 26-6
  - disabled 26-7
  - forwarding 26-5, 26-6
  - learning 26-6
  - listening 26-6
  - overview 26-4
- interoperability and compatibility among modes 26-10
- Layer 2 protocol tunneling 16-8
- limitations with IEEE 802.1Q trunks 26-10
STP (continued)
load sharing
overview 13-24
using path costs 13-26
using port priorities 13-25
loop guard
described 18-9
enabling 18-16
modes supported 26-9
multicast addresses, effect of 26-8
optional features supported 1-8
overview 26-2
path costs 13-26, 13-27
Port Fast
described 18-2
enabling 18-10
port priorities 13-25
preventing root switch selection 18-8
protocols supported 26-9
redundant connectivity 26-8
root guard
described 18-8
enabling 18-16
root port, defined 26-3
root switch
configuring 26-15
effects of extended system ID 26-4, 26-14
election 26-3
unexpected behavior 26-15
shutdown Port Fast-enabled port 18-2
status, displaying 26-22
superior BPDUs 26-3
timers, described 26-20
UplinkFast
described 18-3
enabling 18-14
VLAN-bridge 26-10
stratum, NTP 6-2
stub areas, OSPF 37-29
stub routing, EIGRP 37-39
subdomains, private VLAN 15-1
subnet mask 37-5
subnet zero 37-6
success response, VMPS 13-28
summer time 6-13
SunNet Manager 1-5
supernet 37-6
supported port-based authentication methods 9-8
SVI autostate exclude
configuring 11-27
defined 11-5
SVI link state 11-5
SVIs
and IP unicast routing 37-3
and router ACLs 33-4
connecting VLANs 11-10
defined 11-4
routing between VLANs 13-2
switch 38-2
switch clustering technology 5-1
See also clusters, switch
switch console port 1-6
Switch Database Management
See SDM
switched packets, ACLs on 33-38
Switched Port Analyzer
See SPAN
switched ports 11-2
switchport backup interface 19-4, 19-5
switchport block multicast command 23-8
switchport block unicast command 23-8
switchport command 11-15
switchport mode dot1q-tunnel command 16-6
switchport protected command 23-7
switch priority
MSTP 17-23
STP 26-19
switch software features 1-1
switch virtual interface
   See SVI
synchronization, BGP 37-46
syslog
   See system message logging
system capabilities TLV 25-2
system clock
   configuring
      daylight saving time 6-13
      manually 6-11
      summer time 6-13
      time zones 6-12
   displaying the time and date 6-12
   overview 6-1
   See also NTP
system description TLV 25-2
system message logging
   default configuration 30-3
   defining error message severity levels 30-8
   disabling 30-4
   displaying the configuration 30-13
   enabling 30-4
   facility keywords, described 30-13
   level keywords, described 30-9
   limiting messages 30-10
   message format 30-2
   overview 30-1
   sequence numbers, enabling and disabling 30-8
   setting the display destination device 30-5
   synchronizing log messages 30-6
syslog facility 1-15
   time stamps, enabling and disabling 30-7
UNIX syslog servers
   configuring the daemon 30-12
   configuring the logging facility 30-12
   facilities supported 30-13
system MTU
   and IS-IS LSPs 37-67
system MTU and IEEE 802.1Q tunneling 16-5
system name
   default configuration 6-15
   default setting 6-15
   manual configuration 6-15
   See also DNS
system name TLV 25-2
system prompt, default setting 6-14, 6-15
system resources, optimizing 7-1
system routing
   IS-IS 37-63
   ISO IGRP 37-63
TACACS+
   accounting, defined 8-11
   authentication, defined 8-11
   authorization, defined 8-11
   configuring
      accounting 8-17
      authentication key 8-13
      authorization 8-16
      login authentication 8-14
   default configuration 8-13
   displaying the configuration 8-18
   identifying the server 8-13
   in clusters 5-15
   limiting the services to the user 8-16
   operation of 8-12
   overview 8-10
   support for 1-11
   tracking services accessed by user 8-17
   tagged packets
      IEEE 802.1Q 16-3
      Layer 2 protocol 16-8
tar files
  creating B-6
  displaying the contents of B-6
  extracting B-7
  image file format B-25
TCAM
  memory consistency check errors
    displaying 48-24
    example 48-24
  memory consistency check routines 1-5, 48-24
  memory consistency integrity 1-5, 48-24
  portions 48-24
  space
    HFTM 48-24
    HQATM 48-24
    unassigned 48-24
TCL script, registering and defining with embedded event manager 32-6
TDR 1-15
Telnet
  accessing management interfaces 2-10
  number of connections 1-6
  setting a password 8-6
  temporary self-signed certificate 8-50
Terminal Access Controller Access Control System Plus
  See TACACS+
terminal lines, setting a password 8-6
ternary content addressable memory
  See TCAM
TFTP
  configuration files
    downloading B-11
    preparing the server B-10
    uploading B-12
  configuration files in base directory 3-8
  configuring for autoconfiguration 3-8
  TFTP (continued)
    image files
      deleting B-28
      downloading B-27
      preparing the server B-26
      uploading B-29
    limiting access by servers 31-16
TFTP server 1-5
  threshold, traffic level 23-2
  threshold monitoring, IP SLAs 42-6
time
  See NTP and system clock
Time Domain Reflector
  See TDR
time-range command 33-16
time ranges in ACLs 33-16
time stamps in log messages 30-7
time zones 6-12
TLVs
  defined 25-1
  LLDP 25-2
  LLDP-MED 25-2
Token Ring VLANs
  support for 13-6
  VTP support 14-4
ToS 1-12
traceroute, Layer 2
  and ARP 48-15
  and CDP 48-15
  broadcast traffic 48-15
  described 48-15
  IP addresses and subnets 48-15
  MAC addresses and VLANs 48-15
  multicast traffic 48-15
  multiple devices on a port 48-16
  unicast traffic 48-15
  usage guidelines 48-15
traceroute command 48-17
  See also IP traceroute
Index

tracked lists
  configuring 43-3
  types 43-3

tracked objects
  by Boolean expression 43-4
  by threshold percentage 43-6
  by threshold weight 43-5

tracking interface line-protocol state 43-2

tracking IP routing state 43-2

tracking process 43-1

track state, tracking IP SLAs 43-9

traffic
  blocking flooded 23-8
  fragmented 33-5
  fragmented IPv6 40-2
  unfragmented 33-5

traffic policing 1-12

traffic suppression 23-2

transmit hold-count
  see STP

transparent mode, VTP 14-3

trap-door mechanism 3-2

traps
  configuring MAC address notification 6-22, 6-24, 6-25
  configuring managers 31-12
  defined 31-3
  enabling 6-22, 6-24, 6-25, 31-12
  notification types 31-12
  overview 31-1, 31-4

troubleshooting
  connectivity problems 48-13, 48-14, 48-16
  CPU utilization 48-25
  detecting unidirectional links 27-1
  displaying crash information 48-23
  PIMv1 and PIMv2 interoperability problems 45-35
  setting packet forwarding 48-20
  SFP security and identification 48-12
  show forward command 48-20
  troubleshooting (continued)
    with CiscoWorks 31-4
    with debug commands 48-19
    with ping 48-13
    with system message logging 30-1
    with traceroute 48-16

trunk failover
  See link-state tracking

trunking encapsulation 1-8

trunk ports
  configuring 13-21
  defined 11-3, 13-3
  encapsulation 13-21, 13-26, 13-27

trunks
  allowed-VLAN list 13-22
  configuring 13-21, 13-26, 13-27
  ISL 13-16
  load sharing
    setting STP path costs 13-26
    using STP port priorities 13-25
  native VLAN for untagged traffic 13-24
  parallel 13-26
  pruning-eligible list 13-23
  to non-DTP device 13-17

trusted boundary for QoS 34-43

trusted port states
  between QoS domains 34-45
  classification options 34-5
  ensuring port security for IP phones 34-43
  support for 1-12
  within a QoS domain 34-41

trustpoints, CA 8-50

tunneling
  defined 16-1
  IEEE 802.1Q 16-1
  Layer 2 protocol 16-8
tunnel ports
  defined 13-4
described 11-3, 16-1
IEEE 802.1Q, configuring 16-6
incompatibilities with other features 16-6
twisted-pair Ethernet, detecting unidirectional links 27-1
type of service
  See ToS

U

UDLD
  configuration guidelines 27-4
default configuration 27-4
  disabling
globally 27-5
  on fiber-optic interfaces 27-5
  per interface 27-5
  echoing detection mechanism 27-2
  enabling
globally 27-5
  per interface 27-5
Layer 2 protocol tunneling 16-10
link-detection mechanism 27-1
neighbor database 27-2
overview 27-1
resetting an interface 27-6
status, displaying 27-6
  support for 1-7
UDP, configuring 37-14
UDP jitter, configuring 42-10
UDP jitter operation, IP SLAs 42-9
unauthorized ports with IEEE 802.1x 9-11
unicast MAC address filtering (continued)
  configuration guidelines 6-27
  described 6-27
unicast storm 23-2
unicast storm control command 23-4
unicast traffic, blocking 23-8
UniDirectional Link Detection protocol
  See UDLD
UNIX syslog servers
  daemon configuration 30-12
  facilities supported 30-13
  message logging configuration 30-12
  unrecognized Type-Length-Value (TLV) support 14-4
upgrading software images
  See downloading
UplinkFast
  described 18-3
  disabling 18-14
  enabling 18-14
  support for 1-7
uploading
  configuration files
    preparing B-10, B-13, B-16
    reasons for B-8
    using FTP B-15
    using RCP B-18
    using TFTP B-12
  image files
    preparing B-26, B-30, B-34
    reasons for B-24
    using FTP B-33
    using RCP B-37
    using TFTP B-29
User Datagram Protocol
  See UDP
user EXEC mode 2-2
username-based authentication 8-7
V

version-dependent transparent mode 14-4
virtual IP address
  cluster standby group 5-12
  command switch 5-12
Virtual Private Network
  See VPN
virtual router 41-1, 41-2
virtual switches and PAgP 35-5
vlan.dat file 13-5
VLAN 1, disabling on a trunk port 13-22
VLAN 1 minimization 13-22
VLAN ACLs
  See VLAN maps
vlan-assignment response, VMPS 13-28
VLAN configuration
  at bootup 13-7
  saving 13-7
VLAN configuration mode 2-2
VLAN database
  and startup configuration file 13-7
  and VTP 14-1
  VLAN configuration saved in 13-7
  VLANs saved in 13-4
vlan dot1q tag native command 16-5
VLAN filtering and SPAN 28-6
vlan global configuration command 13-7
VLAN ID, discovering 6-30
VLAN link state 11-5
VLAN load balancing on flex links 19-3
  configuration guidelines 19-8
VLAN management domain 14-2
VLAN Management Policy Server
  See VMPS
VLAN map entries, order of 33-30

VLAN maps
  applying 33-34
  common uses for 33-34
  configuration guidelines 33-30
  configuring 33-29
  creating 33-31
  defined 33-2
  denying access to a server example 33-35
  denying and permitting packets 33-31
  displaying 33-41
  examples of ACLs and VLAN maps 33-32
  removing 33-34
  support for 1-10
  wiring closet configuration example 33-35
VLAN membership
  confirming 13-31
  modes 13-3
VLAN Query Protocol
  See VQP
VLANs
  adding 13-8
  adding to VLAN database 13-8
  aging dynamic addresses 26-9
  allowed on trunk 13-22
  and spanning-tree instances 13-3, 13-6, 13-11
  configuration guidelines, extended-range VLANs 13-11
  configuration guidelines, normal-range VLANs 13-6
  configuring 13-1
  configuring IDs 1006 to 4094 13-11
  connecting through SVIs 11-10
  creating 13-8
  customer numbering in service-provider networks 16-3
  default configuration 13-7
  deleting 13-9
  described 11-2, 13-1
  displaying 13-15
  extended-range 13-1, 13-11
VLANs (continued)

features 1-8
illustrated 13-2
internal 13-12
limiting source traffic with RSPAN 28-22
limiting source traffic with SPAN 28-15
modifying 13-8
multicast 22-18
native, configuring 13-24
normal-range 13-1, 13-4
number supported 1-8
parameters 13-5
port membership modes 13-3
static-access ports 13-9
STP and IEEE 802.1Q trunks 26-10
supported 13-2
Token Ring 13-6
traffic between 13-2
VLAN-bridge STP 26-10, 47-2
VTP modes 14-3

VLAN Trunking Protocol
See VTP

VLAN trunks 13-16

VMPS
administering 13-33
configuration example 13-33
configuration guidelines 13-29
default configuration 13-29
description 13-28
dynamic port membership
described 13-29
reconfirming 13-32
troubleshooting 13-33
entering server address 13-30
mapping MAC addresses to VLANs 13-28
monitoring 13-33
reconfirmation interval, changing 13-32
reconfirming membership 13-31
retry count, changing 13-32
voice aware 802.1x security
port-based authentication
configuring 9-40
described 9-32, 9-40
voice-over-IP 12-1
voice VLAN
Cisco 7960 phone, port connections 12-1
configuration guidelines 12-3
configuring IP phones for data traffic
override CoS of incoming frame 12-7
trust CoS priority of incoming frame 12-7
configuring ports for voice traffic in
802.1p priority tagged frames 12-6
802.1Q frames 12-5
connecting to an IP phone 12-5
default configuration 12-3
described 12-1
displaying 12-8
IP phone data traffic, described 12-3
IP phone voice traffic, described 12-2
VPN
configuring routing in 37-82
forwarding 37-75
in service provider networks 37-72
routes 37-73
VPN routing and forwarding table
See VRF
VQP 1-8, 13-28
VRF
defining 37-75
tables 37-72
VRF-aware services
ARP 37-79
configuring 37-78
ftp 37-81
HSRP 37-80
ping 37-79
RADIUS 37-80
SNMP 37-79
VRF-aware services (continued)
  syslog 37-80
  tftp 37-81
  traceroute 37-81
VTP
  adding a client to a domain 14-15
  advertisements 13-19, 14-3, 14-4
  and extended-range VLANs 13-3, 14-1
  and normal-range VLANs 13-2, 14-1
  client mode, configuring 14-12
  configuration
    guidelines 14-8
    requirements 14-10
    saving 14-8
  configuration requirements 14-10
  configuration revision number
    guideline 14-15
    resetting 14-16
  consistency checks 14-4
  default configuration 14-7
  described 14-1
  domain names 14-8
  domains 14-2
  Layer 2 protocol tunneling 16-8
  modes
    client 14-3
    off 14-3
    server 14-3
    transitions 14-3
    transparent 14-3
  monitoring 14-16
  passwords 14-8
  pruning
    disabling 14-14
    enabling 14-14
    examples 14-6
    overview 14-5
    support for 1-8
    pruning-eligible list, changing 13-23
VTP (continued)
  server mode, configuring 14-10, 14-13
  statistics 14-16
  support for 1-8
  Token Ring support 14-4
  transparent mode, configuring 14-10
  using 14-1
  Version
    enabling 14-13
    version, guidelines 14-9
  Version 1 14-4
  Version 2
    configuration guidelines 14-9
    overview 14-4
  Version 3
    overview 14-5
W
WCCP
  authentication 44-3
  configuration guidelines 44-5
  default configuration 44-5
  described 44-1
  displaying 44-9
  dynamic service groups 44-3
  enabling 44-6
  features unsupported 44-4
  forwarding method 44-3
  Layer-2 header rewrite 44-3
  MD5 security 44-3
  message exchange 44-2
  negotiation 44-3
  packet redirection 44-3
  packet-return method 44-3
  redirecting traffic received from a client 44-6
  setting the password 44-6
  unsupported WCCPv2 features 44-4
web authentication 9-17
  configuring 10-16 to ??
  described 1-9
web-based authentication
  customizeable web pages 10-6
  description 10-1
web-based authentication, interactions with other features 10-7
Web Cache Communication Protocol
  See WCCP
weighted tail drop
  See WTD
weight thresholds in tracked lists 43-5
wired location service
  configuring 25-10
  displaying 25-12
  location TLV 25-3
  understanding 25-3
wizards 1-2
WTD
  described 34-14
  setting thresholds
    egress queue-sets 34-78
    ingress queues 34-73
  support for 1-13

X

Xmodem protocol 48-2
Preface

Audience

This guide is for the networking professional managing the Catalyst 3560 switch, hereafter referred to as the switch. Before using this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

The Catalyst 3560 switch is supported by either the IP base image or the IP services image. The IP base image provides Layer 2+ features including access control lists (ACLs), quality of service (QoS), static routing, EIGRP stub routing, and the Routing Information IP services image provides a richer set of enterprise-class features. It includes Layer 2+ features and full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging). To distinguish it from the Layer 2+ static routing and RIP, the IP services image includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and the Open Shortest Path First (OSPF) Protocol.

This guide provides procedures for using the commands that have been created or changed for use with the switch. It does not provide detailed information about these commands. For detailed information about these commands, see the Catalyst 3560 Switch Command Reference for this release. For information about the standard Cisco IOS Release 12.2 commands, see the Cisco IOS documentation set available from the Cisco.com home page at Documentation > Cisco IOS Software.

This guide does not provide detailed information on the graphical user interfaces (GUIs) for the embedded device manager or for Cisco Network Assistant (hereafter referred to as Network Assistant) that you can use to manage the switch. However, the concepts in this guide are applicable to the GUI user. For information about the device manager, see the switch online help. For information about Network Assistant, see Getting Started with Cisco Network Assistant, available on Cisco.com.

This guide does not describe system messages you might encounter or how to install your switch. For more information, see the Catalyst 3560 Switch System Message Guide for this release and the Catalyst 3560 Switch Hardware Installation Guide.

For documentation updates, see the release notes for this release.
Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:
- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars ( | ) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:
- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **boldface** `screen` font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and timesavers use these conventions and symbols:

| ![Note] | Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual. |
| ![Caution] | Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data. |

Related Publications

These documents provide complete information about the switch and are available from this Cisco.com site:

| ![Note] | Before installing, configuring, or upgrading the switch, see these documents: |
| | - For initial configuration information, see the “Using Express Setup” section in the getting started guide or the “Configuring the Switch with the CLI-Based Setup Program” appendix in the hardware installation guide. |
| | - For device manager requirements, see the “System Requirements” section in the release notes (not orderable but available on Cisco.com). |
| | - For Network Assistant requirements, see the Getting Started with Cisco Network Assistant (not orderable but available on Cisco.com). |
| | - For cluster requirements, see the Release Notes for Cisco Network Assistant (not orderable but available on Cisco.com). |
| | - For upgrading information, see the “Downloading Software” section in the release notes. |
See these documents for other information about the switch:

- Release Notes for the Catalyst 3750, 3560, 2975, and 2960 Switches
- Catalyst 3750, 3560, 3550, 2975, 2975, 2970, and 2960 and 2960-S Switch System Message Guide
- Catalyst 3560 Switch Software Configuration Guide
- Catalyst 3560 Switch Command Reference
- Device manager online help (available on the switch)
- Catalyst 3560 Switch Hardware Installation Guide
- Catalyst 3560 Switch Getting Started Guide
- Regulatory Compliance and Safety Information for the Catalyst 3560 Switch
- Auto Smartports Configuration Guide
- Cisco EnergyWise Configuration Guide
- Getting Started with Cisco Network Assistant
- Release Notes for Cisco Network Assistant
- Cisco CWDM GBIC and CWDM SFP Installation Note
- Cisco RPS 300 Redundant Power System Hardware Installation Guide
- Cisco RPS 675 Redundant Power System Hardware Installation Guide
- Cisco Redundant Power System 2300 Hardware Installation Guide
- For information about the Network Admission Control (NAC) features, see the Network Admission Control Software Configuration Guide

**Obtaining Documentation, Obtaining Support, and Security Guidelines**

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: [http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html](http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html)

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

This chapter provides these topics about the Catalyst 3560 switch software:

- Features, page 1-1
- Default Settings After Initial Switch Configuration, page 1-16
- Network Configuration Examples, page 1-19
- Where to Go Next, page 1-26

In this document, IP refers to IP Version 4 (IPv4) unless there is a specific reference to IP Version 6 (IPv6).

Features

The switch ships with one of these software images installed:

- IP base image, which provides Layer 2+ features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, EIGRP stub routing, PIM stub routing, the Hot Standby Router Protocol (HSRP), and the Routing Information Protocol (RIP). Switches with the IP base image installed can be upgraded to IP services image.

- IP services image, which provides a richer set of enterprise-class intelligent services. It includes all IP base image features plus full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging). To distinguish it from the Layer 2+ static routing and RIP, the IP services image includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and the Open Shortest Path First (OSPF) Protocol.

IPv6 Multicast Listener Discovery (MLD) snooping is supported in all Catalyst 3560 and 3750 images; for more information, see Chapter 39, “Configuring IPv6 MLD Snooping.”

For full IPv6 support, the IP services image is required. For more information on IPv6 routing, see Chapter 38, “Configuring IPv6 Unicast Routing.”

For information on IPv6 ACLs, see Chapter 40, “Configuring IPv6 ACLs.”
Some features described in this chapter are available only on the cryptographic (supports encryption) version of the software. You must obtain authorization to use this feature and to download the cryptographic version of the software from Cisco.com. For more information, see the release notes for this release.

- **Ease-of-Deployment and Ease-of-Use Features**, page 1-2
- **Performance Features**, page 1-3
- **Management Options**, page 1-5
- **Manageability Features**, page 1-5
- **Availability and Redundancy Features**, page 1-7
- **VLAN Features**, page 1-8
- **Security Features**, page 1-9
- **QoS and CoS Features**, page 1-12
- **Layer 3 Features**, page 1-13 (includes features requiring the IP services image)
- **Power over Ethernet Features**, page 1-14
- **Monitoring Features**, page 1-15

### Ease-of-Deployment and Ease-of-Use Features

- **Express Setup** for quickly configuring a switch for the first time with basic IP information, contact information, switch and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see the getting started guide.

- **User-defined and Cisco-default Smartports macros** for creating custom switch configurations for simplified deployment across the network.

- **An embedded device manager GUI** for configuring and monitoring a single switch through a web browser. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.

- **Cisco Network Assistant** (hereafter referred to as *Network Assistant*) for
  - Managing communities, which are device groups like clusters, except that they can contain routers and access points and can be made more secure.
  - Simplifying and minimizing switch and switch cluster management from anywhere in your intranet.
  - Accomplishing multiple configuration tasks from a single graphical interface without needing to remember command-line interface (CLI) commands to accomplish specific tasks.
  - Interactive guide mode that guides you in configuring complex features such as VLANs, ACLs, and quality of service (QoS).
  - Configuration wizards that prompt you to provide only the minimum required information to configure complex features such as QoS priorities for traffic, priority levels for data applications, and security.
  - Downloading an image to a switch.
  - Applying actions to multiple ports and multiple switches at the same time, such as VLAN and QoS settings, inventory and statistic reports, link- and switch-level monitoring and troubleshooting, and multiple switch software upgrades.
– Viewing a topology of interconnected devices to identify existing switch clusters and eligible switches that can join a cluster and to identify link information between switches.

– Monitoring real-time status of a switch or multiple switches from the LEDs on the front-panel images. The system, redundant power system (RPS), and port LED colors on the images are similar to those used on the physical LEDs.

**Note**
The Network Assistant must be downloaded from cisco.com/go/cna.

- Switch clustering technology for
  - Unified configuration, monitoring, authentication, and software upgrade of multiple, cluster-capable switches, regardless of their geographic proximity and interconnection media, including Ethernet, Fast Ethernet, Fast EtherChannel, small form-factor pluggable (SFP) modules, Gigabit Ethernet, and Gigabit EtherChannel connections. For a list of cluster-capable switches, see the release notes.
  - Automatic discovery of candidate switches and creation of clusters of up to 16 switches that can be managed through a single IP address.
  - Extended discovery of cluster candidates that are not directly connected to the command switch.

- Auto Smartports
  - Cisco-default and user-defined macros for dynamic port configuration based on the device type detected on the port.
  - Enhancements to add support for global macros, last-resort macros, event trigger control, access points, EtherChannels, auto-QoS with Cisco Medianet, and IP phones.
  - Enhancements to add support for macro persistency, LLDP-based triggers, MAC address and OUI-based triggers, remote macros as well as for automatic configuration based on these two new device types: Cisco Digital Media Player (Cisco DMP) and Cisco IP Video Surveillance Camera (Cisco IPVSC).

For information, see the *Auto Smartports Configuration Guide*.

- Smart Install to allow a single point of management (director) in a network. You can use Smart Install to provide zero touch image and configuration upgrade of newly deployed switches and image and configuration downloads for any client switches. For more information, see the *Cisco Smart Install Configuration Guide*.

- Smart Install enhancements in Cisco IOS Release 12.2(55)SE supporting client backup files, zero-touch replacement for clients with the same product-ID, automatic generation of the image list file, configurable file repository, hostname changes, transparent connection of the director to client, and USB storage for image and seed configuration.

### Performance Features

- Cisco EnergyWise manages the energy usage of end points including power over Ethernet (PoE) devices and non-Cisco devices. For information, see the *Cisco EnergyWise Configuration Guide*.

- Autosensing of port speed and autonegotiation of duplex mode on all switch ports for optimizing bandwidth.
• Automatic-medium-dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 Mb/s interfaces and on 10/100/1000 BASE-TX SFP module interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately.

• Support for up to 1546 bytes routed frames, up to 9000 bytes for frames that are bridged in hardware, and up to 2000 bytes for frames that are bridged by software.

• IEEE 802.3x flow control on all ports (the switch does not send pause frames).

• EtherChannel for enhanced fault tolerance and for providing up to 8 Gb/s (Gigabit EtherChannel) or 800 Mb/s (Fast EtherChannel) full-duplex bandwidth among switches, routers, and servers.

• Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links.

• Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate

• Multicast virtual routing and forwarding (VRF) Lite for configuring multiple private routing domains for network virtualization and virtual private multicast networks

• Per-port storm control for preventing broadcast, multicast, and unicast storms.

• Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic.

• Cisco Group Management Protocol (CGMP) server support and Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3:
  – (For CGMP devices) CGMP for limiting multicast traffic to specified end stations and reducing overall network traffic.
  – (For IGMP devices) IGMP snooping for forwarding multimedia and multicast traffic.

• IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries).

• IGMP snooping querier support to configure switch to generate periodic IGMP general query messages.

• IGMP helper to allow the switch to forward a host request to join a multicast stream to a specific IP destination address.

• Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.

• IGMP filtering for controlling the set of multicast groups to which hosts on a switch port can belong.

• IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table.

• IGMP leave timer for configuring the leave latency for the network.

• Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features.

• Web Cache Communication Protocol (WCCP) for redirecting traffic to local wide-area application engines, for enabling content requests to be fulfilled locally, and for localizing web-traffic patterns in the network (requires the IP services image).

• Cisco IOS IP Service Level Agreements (SLAs), a part of Cisco IOS software that uses active traffic monitoring for measuring network performance.

• Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold).
• Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure.
• RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
• Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports.
• Support for QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports.
• Memory consistency check routines to detect and correct invalid ternary content addressable memory (TCAM) table entries.

Management Options

• An embedded device manager—The device manager is a GUI that is integrated in the software image. You use it to configure and to monitor a single switch. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
• Network Assistant—Network Assistant is a network management application that can be downloaded from Cisco.com. You use it to manage a single switch, a cluster of switches, or a community of devices. For more information about Network Assistant, see Getting Started with Cisco Network Assistant, available on Cisco.com.
• CLI—The Cisco IOS software supports desktop- and multilayer-switching features. You can access the CLI by connecting your management station directly to the switch console port, by connecting your PC directly to the Ethernet management port, or by using Telnet from a remote management station or PC. For more information about the CLI, see Chapter 2, “Using the Command-Line Interface.”
• SNMP—SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch supports a comprehensive set of MIB extensions and four remote monitoring (RMON) groups. For more information about using SNMP, see Chapter 31, “Configuring SNMP.”
• Cisco IOS Configuration Engine (previously known to as the Cisco IOS CNS agent) — Configuration service automates the deployment and management of network devices and services. You can automate initial configurations and configuration updates by generating switch-specific configuration changes, sending them to the switch, executing the configuration change, and logging the results.
For more information about CNS, see Chapter 4, “Configuring Cisco IOS Configuration Engine.”

Manageability Features

• CNS embedded agents for automating switch management, configuration storage, and delivery
• DHCP for automating configuration of switch information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
• DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
• DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
• DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches
• DHCP server port-based address allocation for the preassignment of an IP address to a switch port
• Directed unicast requests to a DNS server for identifying a switch through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server
• Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding MAC address
• Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
• Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table
• Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network
• Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones
• LLDP media extensions (LLDP-MED) location TLV that provides location information from the switch to the endpoint device
• Support for CDP and LLDP enhancements for exchanging location information with video endpoints for dynamic location-based content distribution from servers
• Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source
• Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch uses
• Support for the SSM PIM protocol to optimize multicast applications, such as video
• Source Specific Multicast (SSM) mapping for multicast applications provides a mapping of source to group, allowing listeners to connect to multicast sources dynamically and reduces dependencies on the application
• Support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 to utilize IPv6 transport, communicate with IPv6 peers, and advertise IPv6 routes
• Support for these IP services, making them VRF aware so that they can operate on multiple routing instances: HSRP, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping
• Configuration logging to log and to view changes to the switch configuration
• Unique device identifier to provide product identification information through a show inventory user EXEC command display
• In-band management access through the device manager over a Netscape Navigator or Microsoft Internet Explorer browser session
• In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
• In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network
• In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
• Out-of-band management access through the switch console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
• Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying switch configuration or switch image files (requires the cryptographic version of the software)
• Configuration replacement and rollback to replace the running configuration on a switch with any saved Cisco IOS configuration file
• The HTTP client in Cisco IOS supports can send requests to both IPv4 and IPv6 HTTP server, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients
• Simple Network and Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can send SNMP queries and receive SNMP notifications from a device running IPv6
• IPv6 stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses
• Disabling MAC address learning on a VLAN
• DHCP server port-based address allocation for the preassignment of an IP address to a switch port.
• Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE)
• CPU utilization threshold trap monitors CPU utilization
• LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode
• Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol
• DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field
• Increased support for LLDP-MED by allowing the switch to grant power to the power device (PD), based on the power policy TLV request

Availability and Redundancy Features

• HSRP for command switch and Layer 3 router redundancy
• Enhanced object tracking, which separates the tracking mechanism from HSRP and creates a separate, standalone tracking process that can be used by processes other than HSRP
• UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
• IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  – Up to 128 spanning-tree instances supported
  – Per-VLAN spanning-tree plus (PVST+) for load balancing across VLANs
  – Rapid PVST+ for load balancing across VLANs and providing rapid convergence of spanning-tree instances
  – UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks
IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state

Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
- Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state
- BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
- BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs
- Root guard for preventing switches outside the network core from becoming the spanning-tree root
- Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link

Equal-cost routing for link-level and switch-level redundancy

Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy

Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another Cisco Ethernet switch.

RPS support through the Cisco Redundant Power System 2300, also referred to as the RPS 2300, for enhancing power reliability, configuring and managing the redundant power system. For more information about the RPS 2300, see the Cisco Redundant Power System 2300 Hardware Installation Guide that shipped with the device and that is also on Cisco.com.

VLAN Features

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the 1 to 4094 range as allowed by the IEEE 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- Inter-Switch Link (ISL) and IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (IEEE 802.1Q or ISL) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
- Voice VLAN for creating subnets for voice traffic from Cisco IP Phones
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch CPU continues to send and receive control protocol frames.
Private VLANs to address VLAN scalability problems, to provide a more controlled IP address allocation, and to allow Layer 2 ports to be isolated from other ports on the switch

Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port

VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

Support for 802.1x authentication with restricted VLANs (also known as authentication failed VLANs)

Support for VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port

Security Features

IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring

IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover

Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser

Local web authentication banner so that a custom banner or an image file can be displayed at a web authentication login screen

MAC authentication bypass (MAB) aging timer to detect inactive hosts that have authenticated after they have authenticated by using MAB

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

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 security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)

Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces

VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers
• Source and destination MAC-based ACLs for filtering non-IP traffic
• IPv6 ACLs to be applied to interfaces to filter IPv6 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 802.1Q tunneling so that customers with users at remote sites across a service-provider network can keep VLANs segregated from other customers and Layer 2 protocol tunneling to ensure that the customer’s network has complete STP, CDP, and VTP information about all users
• Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels
• Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors
• IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:
  – Multidomain authentication (MDA) to allow both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to independently authenticate on the same IEEE 802.1x-enabled switch port
  – Dynamic voice virtual LAN (VLAN) for MDA to allow a dynamic voice VLAN on an MDA-enabled port
  – VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN
  – Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.
  – Port security for controlling access to 802.1x ports
  – Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port
  – IP phone detection enhancement to detect and recognize a Cisco IP phone.
  – Guest VLAN to provide limited services to non-802.1x-compliant users
  – Restricted VLAN to provide limited services to users who are 802.1x compliant, but do not have the credentials to authenticate via the standard 802.1x processes
  – 802.1x accounting to track network usage
  – 802.1x 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 to authorize clients based on the client MAC address.
  – 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 Cisco Secure ACS server to an authenticated switch.
- Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs.
- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.
- Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port.

- Network Admission Control (NAC) features:
  - NAC Layer 2 802.1x validation of the antivirus condition or posture of endpoint systems or clients before granting the devices network access.
    For information about configuring NAC Layer 2 802.1x validation, see the “Configuring NAC Layer 2 802.1x Validation” section on page 10-61.
  - NAC Layer 2 IP validation of the posture of endpoint systems or clients before granting the devices network access.
    For information about configuring NAC Layer 2 IP validation, see the Network Admission Control Software Configuration Guide.
  - IEEE 802.1x inaccessible authentication bypass.
    For information about configuring this feature, see the “Configuring Inaccessible Authentication Bypass and Critical Voice VLAN” section on page 10-56.
  - Authentication, authorization, and accounting (AAA) down policy for a NAC Layer 2 IP validation of a host if the AAA server is not available when the posture validation occurs.
    For information about this feature, see the Network Admission Control Software Configuration Guide.

- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through AAA services
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic versions of the software)
- 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)
- Voice aware IEEE 802.1x and MAC authentication bypass (MAB) security violation to shut down only the data VLAN on a port when a security violation occurs
- Support for IP source guard on static hosts.
- RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco 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 with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.

• Customizable web authentication enhancement to allow the creation of user-defined login, success, failure and expire web pages for local web authentication.

• Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.

• VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.

• MAC move to allow hosts (including the hosts connected behind an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.

• Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.

• Support for the Security Group Tag (SCT) Exchange Protocol (SXP) component of Cisco TrustSec, a security architecture using authentication, encryption, and access control.

QoS and CoS Features

• Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues

• Automatic quality of service (QoS) Voice over IP (VoIP) enhancement for port-based trust of DSCP and priority queuing for egress traffic

• Classification
  – IP type-of-service/Differentiated Services Code Point (IP ToS/DSCP) and IEEE 802.1p CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications
  – IP ToS/DSCP and IEEE 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network
  – Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain
  – Trusted boundary for detecting the presence of a Cisco IP Phone, trusting the CoS value received, and ensuring port security

• Policing
  – Traffic-policing policies on the switch port for managing how much of the port bandwidth should be allocated to a specific traffic flow
  – If you configure multiple class maps for a hierarchical policy map, each class map can be associated with its own port-level (second-level) policy map. Each second-level policy map can have a different policer.
  – Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates
Features

- Out-of-Profile
  - Out-of-profile markdown for packets that exceed bandwidth utilization limits
- Ingress queueing and scheduling
  - Two configurable ingress queues for user traffic (one queue can be the priority queue)
  - Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - Shaped round robin (SRR) as the scheduling service for specifying the rate at which packets are sent to the internal ring (sharing is the only supported mode on ingress queues)
- Egress queues and scheduling
  - Four egress queues per port
  - WTD as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - SRR as the scheduling service for specifying the rate at which packets are dequeued to the egress interface (shaping or sharing is supported on egress queues). Shaped egress queues are guaranteed but limited to using a share of port bandwidth. Shared egress queues are also guaranteed a configured share of bandwidth, but can use more than the guarantee if other queues become empty and do not use their share of the bandwidth.
- Support for IPv6 QoS trust capability.
- Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices, such as the Cisco Telepresence System and Cisco Surveillance Camera.

Layer 3 Features

Note

Some features noted in this section are available only on the IP services image.

- HSRP Version 1 (HSRPv1) and HSRP Version 2 (HSRPv2) for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - Full OSPF (requires the IP services feature set)
    Starting with Cisco IOS Release 12.2(55)SE, the IP base feature set supports OSPF for routed access to enable customers to extend Layer 3 routing capabilities to the access or wiring closet.
  - Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 to utilize IPv6 transport, communicate with IPv6 peers, and advertise IPv6 routes
  - HSRP for IPv6 (requires the IP services image)
  - Border Gateway Protocol (BGP) Version 4 (requires the IP services image)
- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Policy-based routing (PBR) for configuring defined policies for traffic flows
- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs (requires the IP services image)
• Fallback bridging for forwarding non-IP traffic between two or more VLANs (requires the IP services image)
• Static IP routing for manually building a routing table of network path information
• Equal-cost routing for load balancing and redundancy
• Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets
• Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode (requires the IP services image)
• Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains (requires the IP services image)
• Distance Vector Multicast Routing Protocol (DVMRP) tunneling for interconnecting two multicast-enabled networks across nonmulticast networks (requires the IP services image)
• DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
• DHCP for IPv6 relay, client, server address assignment and prefix delegation
• IPv6 unicast routing capability for forwarding IPv6 traffic through configured interfaces (requires the IP services image)
• IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router
• Nonstop forwarding (NSF) awareness to enable the Layer 3 switch to continue forwarding packets from an NSF-capable neighboring router when the primary route processor (RP) is failing and the backup RP is taking over, or when the primary RP is manually reloaded for a nondisruptive software upgrade (requires the IP services image)
• The ability to exclude a port in a VLAN from the SVI line-state up or down calculation

Power over Ethernet Features

• Ability to provide power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices from Power over Ethernet (PoE)-capable ports if the switch detects that there is no power on the circuit.
• Support for CDP with power consumption. The powered device notifies the switch of the amount of power it is consuming.
• Support for Cisco intelligent power management. The powered device and the switch negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power Cisco powered device to operate at its highest power mode.
• Automatic detection and power budgeting; the switch maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.
Monitoring Features

- EOT and IP SLAs EOT static route support identify when a preconfigured static route or a DHCP route goes down
- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them through a policy
- Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.
- Switch LEDs that provide port- and switch-level status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN
- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device
- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on 10/100/1000 copper Ethernet ports
- SFP module diagnostic management interface to monitor physical or operational status of an SFP module
- Generic online diagnostics to test hardware functionality of the supervisor engine, modules, and switch while the switch is connected to a live network.
- On-board failure logging (OBFL) to collect information about the switch and the power supplies connected to it (Catalyst 2960-S only)
- Enhanced object tracking for HSRP.
- Digital optical monitoring (DOM) to check status of X2 small form-factor pluggable (SFP) modules
Default Settings After Initial Switch Configuration

The switch is designed for plug-and-play operation, requiring only that you assign basic IP information to the switch and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

Note

For information about assigning an IP address by using the browser-based Express Setup program, see the getting started guide. For information about assigning an IP address by using the CLI-based setup program, see the hardware installation guide.

If you do not configure the switch at all, the switch operates with these default settings:

- Default switch IP address, subnet mask, and default gateway is 0.0.0.0. For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway,” and Chapter 20, “Configuring DHCP Features and IP Source Guard Features.”
- Default domain name is not configured. For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway.”
- DHCP client is enabled, the DHCP server is enabled (only if the device acting as a DHCP server is configured and is enabled), and the DHCP relay agent is enabled (only if the device is acting as a DHCP relay agent is configured and is enabled). For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway,” and Chapter 20, “Configuring DHCP Features and IP Source Guard Features.”
- Switch cluster is disabled. For more information about switch clusters, see Chapter 5, “Clustering Switches,” and the Getting Started with Cisco Network Assistant, available on Cisco.com.
- No passwords are defined. For more information, see Chapter 6, “Administering the Switch.”
- System name and prompt is Switch. For more information, see Chapter 6, “Administering the Switch.”
- NTP is enabled. For more information, see Chapter 6, “Administering the Switch.”
- DNS is enabled. For more information, see Chapter 6, “Administering the Switch.”
- TACACS+ is disabled. For more information, see Chapter 8, “Configuring Switch-Based Authentication.”
- RADIUS is disabled. For more information, see Chapter 8, “Configuring Switch-Based Authentication.”
- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see Chapter 8, “Configuring Switch-Based Authentication.”
- IEEE 802.1x is disabled. For more information, see Chapter 10, “Configuring IEEE 802.1x Port-Based Authentication.”
- Port parameters
  - Operating mode is Layer 2 (switchport). For more information, see Chapter 11, “Configuring Interface Characteristics.”
  - Interface speed and duplex mode is autonegotiate. For more information, see Chapter 11, “Configuring Interface Characteristics.”
  - Auto-MDIX is enabled. For more information, see Chapter 11, “Configuring Interface Characteristics.”
– Flow control is off. For more information, see Chapter 11, “Configuring Interface Characteristics.”
– PoE is autonegotiate. For more information, see Chapter 11, “Configuring Interface Characteristics.”

- **VLANs**
  – Default VLAN is VLAN 1. For more information, see Chapter 13, “Configuring VLANs.”
  – VLAN trunking setting is dynamic auto (DTP). For more information, see Chapter 13, “Configuring VLANs.”
  – Trunk encapsulation is negotiate. For more information, see Chapter 13, “Configuring VLANs.”
  – VTP mode is server. For more information, see Chapter 14, “Configuring VTP.”
  – VTP version is Version 1. For more information, see Chapter 14, “Configuring VTP.”
  – No private VLANs are configured. For more information, see Chapter 15, “Configuring Private VLANs.”
  – Voice VLAN is disabled. For more information, see Chapter 12, “Configuring Voice VLAN.”

- **IEEE 802.1Q tunneling and Layer 2 protocol tunneling** are disabled. For more information, see Chapter 16, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

- **STP, PVST+** is enabled on VLAN 1. For more information, see Chapter 26, “Configuring STP.”
- **MSTP** is disabled. For more information, see Chapter 17, “Configuring MSTP.”
- **Optional spanning-tree features** are disabled. For more information, see Chapter 18, “Configuring Optional Spanning-Tree Features.”
- **Flex Links** are not configured. For more information, see Chapter 19, “Configuring Flex Links and the MAC Address-Table Move Update Feature.”

- **DHCP snooping** is disabled. The DHCP snooping information option is enabled. For more information, see Chapter 20, “Configuring DHCP Features and IP Source Guard Features.”
- **IP source guard** is disabled. For more information, see Chapter 20, “Configuring DHCP Features and IP Source Guard Features.”
- **DHCP server port-based address allocation** is disabled. For more information, see Chapter 20, “Configuring DHCP Features and IP Source Guard Features.”
- **Dynamic ARP inspection** is disabled on all VLANs. For more information, see Chapter 21, “Configuring Dynamic ARP Inspection.”
- **IGMP snooping** is enabled. No IGMP filters are applied. For more information, see Chapter 22, “Configuring IGMP Snooping and MVR.”
- **IGMP throttling setting** is deny. For more information, see Chapter 22, “Configuring IGMP Snooping and MVR.”
- The IGMP snooping querier feature is disabled. For more information, see Chapter 22, “Configuring IGMP Snooping and MVR.”
- **MVR** is disabled. For more information, see Chapter 22, “Configuring IGMP Snooping and MVR.”
• Port-based traffic
  – Broadcast, multicast, and unicast storm control is disabled. For more information, see Chapter 23, “Configuring Port-Based Traffic Control.”
  – No protected ports are defined. For more information, see Chapter 23, “Configuring Port-Based Traffic Control.”
  – Unicast and multicast traffic flooding is not blocked. For more information, see Chapter 23, “Configuring Port-Based Traffic Control.”
  – No secure ports are configured. For more information, see Chapter 23, “Configuring Port-Based Traffic Control.”

• CDP is enabled. For more information, see Chapter 24, “Configuring CDP.”

• UDLD is disabled. For more information, see Chapter 27, “Configuring UDLD.”

• SPAN and RSPAN are disabled. For more information, see Chapter 28, “Configuring SPAN and RSPAN.”

• RMON is disabled. For more information, see Chapter 29, “Configuring RMON.”

• Syslog messages are enabled and appear on the console. For more information, see Chapter 30, “Configuring System Message Logging.”

• SNMP is enabled (Version 1). For more information, see Chapter 31, “Configuring SNMP.”

• No ACLs are configured. For more information, see Chapter 33, “Configuring Network Security with ACLs.”

• QoS is disabled. For more information, see Chapter 34, “Configuring QoS.”

• No EtherChannels are configured. For more information, see Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

• IP unicast routing is disabled. For more information, see Chapter 37, “Configuring IP Unicast Routing.”

• IPv6 unicast routing is disabled. For more information, see Chapter 38, “Configuring IPv6 Unicast Routing.”

• No HSRP groups are configured. For more information, see Chapter 41, “Configuring HSRP.”

• IP multicast routing is disabled on all interfaces. For more information, see Chapter 45, “Configuring IP Multicast Routing.”

• MSDP is disabled. For more information, see Chapter 46, “Configuring MSDP.”

• Fallback bridging is not configured. For more information, see Chapter 47, “Configuring Fallback Bridging.”
Network Configuration Examples

This section provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections.

- “Design Concepts for Using the Switch” section on page 1-19
- “Small to Medium-Sized Network Using Catalyst 3560 Switches” section on page 1-23
- “Large Network Using Catalyst 3560 Switches” section on page 1-24
- “Long-Distance, High-Bandwidth Transport Configuration” section on page 1-26

Design Concepts for Using the Switch

As your network users compete for network bandwidth, it takes longer to send and receive data. When you configure your network, consider the bandwidth required by your network users and the relative priority of the network applications that they use.

Table 1-1 describes what can cause network performance to degrade and how you can configure your network to increase the bandwidth available to your network users.

<table>
<thead>
<tr>
<th>Network Demands</th>
<th>Suggested Design Methods</th>
</tr>
</thead>
</table>
| Too many users on a single network segment and a growing number of users accessing the Internet | • Create smaller network segments so that fewer users share the bandwidth, and use VLANs and IP subnets to place the network resources in the same logical network as the users who access those resources most.  
• Use full-duplex operation between the switch and its connected workstations. |
| • Increased power of new PCs, workstations, and servers  
• High bandwidth demand from networked applications (such as e-mail with large attached files) and from bandwidth-intensive applications (such as multimedia) | • Connect global resources—such as servers and routers to which the network users require equal access—directly to the high-speed switch ports so that they have their own high-speed segment.  
• Use the EtherChannel feature between the switch and its connected servers and routers. |

Bandwidth alone is not the only consideration when designing your network. As your network traffic profiles evolve, consider providing network services that can support applications for voice and data integration, multimedia integration, application prioritization, and security. Table 1-2 describes some network demands and how you can meet them.
Table 1-2 Providing Network Services

<table>
<thead>
<tr>
<th>Network Demands</th>
<th>Suggested Design Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficient bandwidth usage for multimedia applications and guaranteed bandwidth for critical applications</td>
<td>• Use IGMP snooping to efficiently forward multimedia and multicast traffic.</td>
</tr>
<tr>
<td></td>
<td>• Use other QoS mechanisms such as packet classification, marking, scheduling, and congestion avoidance to classify traffic with the appropriate priority level, thereby providing maximum flexibility and support for mission-critical, unicast, and multicast and multimedia applications.</td>
</tr>
<tr>
<td></td>
<td>• Use optional IP multicast routing to design networks better suited for multicast traffic.</td>
</tr>
<tr>
<td></td>
<td>• Use MVR to continuously send multicast streams in a multicast VLAN but to isolate the streams from subscriber VLANs for bandwidth and security reasons.</td>
</tr>
<tr>
<td>High demand on network redundancy and availability to provide always on mission-critical applications</td>
<td>• Use Hot Standby Router Protocol (HSRP) for cluster command switch and router redundancy.</td>
</tr>
<tr>
<td></td>
<td>• Use VLAN trunks and BackboneFast for traffic-load balancing on the uplink ports so that the uplink port with a lower relative port cost is selected to carry the VLAN traffic.</td>
</tr>
<tr>
<td>An evolving demand for IP telephony</td>
<td>• Use QoS to prioritize applications such as IP telephony during congestion and to help control both delay and jitter within the network.</td>
</tr>
<tr>
<td></td>
<td>• Use switches that support at least two queues per port to prioritize voice and data traffic as either high- or low-priority, based on IEEE 802.1p/Q. The switch supports at least four queues per port.</td>
</tr>
<tr>
<td></td>
<td>• Use voice VLAN IDs (VVIDs) to provide separate VLANs for voice traffic.</td>
</tr>
<tr>
<td>A growing demand for using existing infrastructure to transport data and voice from a home or office to the Internet or an intranet at higher speeds</td>
<td>Use the Catalyst Long-Reach Ethernet (LRE) switches to provide up to 15 Mb of IP connectivity over existing infrastructure, such as existing telephone lines.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> LRE is the technology used in the Catalyst 2900 LRE XL and Catalyst 2950 LRE switches. See the documentation sets specific to these switches for LRE information.</td>
</tr>
</tbody>
</table>
You can use the switches to create the following:

- Cost-effective Gigabit-to-the-desktop for high-performance workgroups (Figure 1-1)—For high-speed access to network resources, you can use the 3560 switches in the access layer to provide Gigabit Ethernet to the desktop. To prevent congestion, use QoS DSCP marking priorities on these switches. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to a Gigabit multilayer switch with routing capability, such as a Catalyst 3750 switch, or to a router.

The first illustration is of an isolated high-performance workgroup, where the Catalyst 3560 switches are connected to Catalyst 3750 switches in the distribution layer. The second illustration is of a high-performance workgroup in a branch office, where the Catalyst 3560 switches are connected to a router in the distribution layer.

Each switch in this configuration provides users with a dedicated 1-Gb/s connection to network resources. Using SFP modules also provides flexibility in media and distance options through fiber-optic connections.

Figure 1-1 High-Performance Workgroup (Gigabit-to-the-Desktop)
Server aggregation (Figure 1-3)—You can use the switches to interconnect groups of servers, centralizing physical security and administration of your network. For high-speed IP forwarding at the distribution layer, connect the switches in the access layer to multilayer switches with routing capability. The Gigabit interconnections minimize latency in the data flow.

QoS and policing on the switches provide preferential treatment for certain data streams. They segment traffic streams into different paths for processing. Security features on the switch ensure rapid handling of packets.

Fault tolerance from the server racks to the core is achieved through dual homing of servers connected to switches, which have redundant Gigabit EtherChannels.

Using dual SFP module uplinks from the switches provides redundant uplinks to the network core. Using SFP modules provides flexibility in media and distance options through fiber-optic connections.
Small to Medium-Sized Network Using Catalyst 3560 Switches

Figure 1-4 shows a configuration for a network of up to 500 employees. This network uses Catalyst 3560 Layer 3 switches with high-speed connections to two routers. For network reliability and load balancing, this network has HSRP enabled on the routers and on the switches. This ensures connectivity to the Internet, WAN, and mission-critical network resources if one of the routers or switches fails. The switches are using routed uplinks for faster failover. They are also configured with equal-cost routing for load sharing and redundancy.

The switches are connected to workstations, local servers, and IEEE 802.3af compliant and noncompliant powered devices (such as Cisco IP Phones). The server farm includes a call-processing server running Cisco CallManager software. Cisco CallManager controls call processing, routing, and Cisco IP Phone features and configuration. The switches are interconnected through Gigabit interfaces.

This network uses VLANs to logically segment the network into well-defined broadcast groups and for security management. Data and multimedia traffic are configured on the same VLAN. Voice traffic from the Cisco IP Phones are configured on separate VVIDs. If data, multimedia, and voice traffic are assigned to the same VLAN, only one VLAN can be configured per wiring closet.

When an end station in one VLAN needs to communicate with an end station in another VLAN, a router or Layer 3 switch routes the traffic to the destination VLAN. In this network, the switches are providing inter-VLAN routing. VLAN access control lists (VLAN maps) on the switch provide intra-VLAN security and prevent unauthorized users from accessing critical areas of the network.

In addition to inter-VLAN routing, the multilayer switches provide QoS mechanisms such as DSCP priorities to prioritize the different types of network traffic and to deliver high-priority traffic. If congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

For prestandard and IEEE 802.3af-compliant powered devices connected to Catalyst PoE switches, IEEE 802.1p/Q QoS gives voice traffic forwarding-priority over data traffic.
Catalyst PoE switch ports automatically detect any Cisco pre-standard and IEEE 802.3af-compliant powered devices that are connected. Each PoE switch port provides 15.4 W of power per port. The powered device, such as a Cisco IP Phone, can receive redundant power when it is also connected to an AC power source. Powered devices not connected to Catalyst PoE switches must be connected to AC power sources to receive power.

Cisco CallManager controls call processing, routing, and Cisco IP Phone features and configuration. Users with workstations running Cisco SoftPhone software can place, receive, and control calls from their PCs. Using Cisco IP Phones, Cisco CallManager software, and Cisco SoftPhone software integrates telephony and IP networks, and the IP network supports both voice and data.

With the multilayer switches providing inter-VLAN routing and other network services, the routers focus on firewall services, Network Address Translation (NAT) services, voice-over-IP (VoIP) gateway services, and WAN and Internet access.

**Figure 1-4  Collapsed Backbone Configuration**

![Collapsed Backbone Configuration Diagram](image)

**Large Network Using Catalyst 3560 Switches**

Switches in the wiring closet have traditionally been only Layer 2 devices, but as network traffic profiles evolve, switches in the wiring closet are increasingly employing multilayer services such as multicast management and traffic classification. Figure 1-5 shows a configuration for a network that only use Catalyst 3560 multilayer switches in the wiring closets and two backbone switches, such as the Catalyst 6500 switches, to aggregate up to ten wiring closets.

In the wiring closet, each switch has IGMP snooping enabled to efficiently forward multimedia and multicast traffic. QoS ACLs that either drop or mark nonconforming traffic based on bandwidth limits are also configured on each switch. VLAN maps provide intra-VLAN security and prevent unauthorized users from accessing critical pieces of the network. QoS features can limit bandwidth on a per-port or
per-user basis. The switch ports are configured as either trusted or untrusted. You can configure a trusted port to trust the CoS value, the DSCP value, or the IP precedence. If you configure the port as untrusted, you can use an ACL to mark the frame in accordance with the network policy.

Each switch provides inter-VLAN routing. They provide proxy ARP services to get IP and MAC address mapping, thereby removing this task from the routers and decreasing this type of traffic on the WAN links. These switches also have redundant uplink connections to the backbone switches, with each uplink port configured as a trusted routed uplink to provide faster convergence in case of an uplink failure.

The routers and backbone switches have HSRP enabled for load balancing and redundant connectivity to guarantee mission-critical traffic.

Figure 1-5  Switches in Wiring Closets in a Backbone Configuration
Long-Distance, High-Bandwidth Transport Configuration

Figure 1-6 shows a configuration for sending 8 Gigabits of data over a single fiber-optic cable. The Catalyst 3560 switches have coarse wavelength-division multiplexing (CWDM) fiber-optic SFP modules installed. Depending on the CWDM SFP module, data is sent at wavelengths from 1470 to 1610 nm. The higher the wavelength, the farther the transmission can travel. A common wavelength used for long-distance transmissions is 1550 nm.

The CWDM SFP modules connect to CWDM optical add/drop multiplexer (OADM) modules over distances of up to 393,701 feet (74.5 miles or 120 km). The CWDM OADM modules combine (or multiplex) the different CWDM wavelengths, allowing them to travel simultaneously on the same fiber-optic cable. The CWDM OADM modules on the receiving end separate (or demultiplex) the different wavelengths.

For more information about the CWDM SFP modules and CWDM OADM modules, see the Cisco CWDM GBIC and CWDM SFP Installation Note.

Where to Go Next

Before configuring the switch, review these sections for startup information:

- Chapter 2, “Using the Command-Line Interface”
- Chapter 3, “Assigning the Switch IP Address and Default Gateway”
Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) and how to use it to configure your Catalyst 3560 switch. Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack.

It contains these sections:

- Understanding Command Modes, page 2-1
- Understanding the Help System, page 2-3
- Understanding Abbreviated Commands, page 2-4
- Understanding no and default Forms of Commands, page 2-4
- Understanding CLI Error Messages, page 2-5
- Using Configuration Logging, page 2-5
- Using Command History, page 2-6
- Using Editing Features, page 2-7
- Searching and Filtering Output of show and more Commands, page 2-10
- Accessing the CLI, page 2-10

Understanding 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.

When you start a session on the switch, 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.
Table 2-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname Switch.

**Table 2-1  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>
<tbody>
<tr>
<td>User EXEC</td>
<td>Begin a session with your switch.</td>
<td>Switch&gt;</td>
<td>Enter <strong>logout</strong> or <strong>quit</strong>.</td>
<td>Use this mode to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Change terminal settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Perform basic tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Display system information.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>While in user EXEC mode, enter the <strong>enable</strong> command.</td>
<td>Switch#</td>
<td>Enter disable to exit.</td>
<td>Use this mode to verify commands that you have entered. Use a password to protect access to this mode.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>While in privileged EXEC mode, enter the <strong>configure</strong> command.</td>
<td>Switch(config)#</td>
<td>To exit to privileged EXEC mode, enter <strong>exit</strong> or <strong>end</strong>, or press <strong>Ctrl-Z</strong>.</td>
<td>Use this mode to configure parameters that apply to the entire switch.</td>
</tr>
<tr>
<td>Config-vlan</td>
<td>While in global configuration mode, enter the <strong>vlan vlan-id</strong> command.</td>
<td>Switch(config-vlan)#</td>
<td>To exit to global configuration mode, enter the <strong>exit</strong> command.</td>
<td>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.</td>
</tr>
<tr>
<td>VLAN configuration</td>
<td>While in privileged EXEC mode, enter the <strong>vlan database</strong> command.</td>
<td>Switch(vlan)#</td>
<td>To exit to privileged EXEC mode, enter <strong>exit</strong>.</td>
<td>Use this mode to configure VLAN parameters for VLANs 1 to 1005 in the VLAN database.</td>
</tr>
</tbody>
</table>
Understanding 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, as shown in Table 2-2.

Table 2-2  Help Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Obtain a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td>abbreviated-command-entry?</td>
<td>Obtain a list of commands that begin with a particular character string.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>Switch# di?</td>
</tr>
<tr>
<td></td>
<td>dir disable disconnect</td>
</tr>
<tr>
<td>abbreviated-command-entry&lt;Tab&gt;</td>
<td>Complete a partial command name.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>Switch# sh conf&lt;tab&gt;</td>
</tr>
<tr>
<td></td>
<td>Switch# show configuration</td>
</tr>
</tbody>
</table>
### 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
```

### Understanding 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 re-enable 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.

---

**Table 2-2  Help Summary (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>?</code></td>
<td>List all commands available for a particular command mode. For example: <code>Switch&gt; ?</code></td>
</tr>
<tr>
<td><code>command ?</code></td>
<td>List the associated keywords for a command. For example: <code>Switch&gt; show ?</code></td>
</tr>
<tr>
<td><code>command keyword ?</code></td>
<td>List the associated arguments for a keyword. For example: <code>Switch(config)# cdp holdtime ?</code></td>
</tr>
</tbody>
</table>

| `<10-255>` | Length of time (in sec) that receiver must keep this packet |
Understanding CLI Error Messages

Table 2-3 lists some error messages that you might encounter while using the CLI to configure your switch.

### Table 2-3 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>Re-enter 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>% Incomplete command.</td>
<td>You did not enter all the keywords or values required by this command.</td>
<td>Re-enter 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 the commands that are available in this command mode. The possible keywords that you can enter with the command appear.</td>
</tr>
</tbody>
</table>

Using 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.

For more information, see the Configuration Change Notification and Logging feature module:


---

**Note**

Only CLI or HTTP changes are logged.
Using 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 as described in these sections:

- **Changing the Command History Buffer Size, page 2-6** (optional)
- **Recalling Commands, page 2-6** (optional)
- **Disabling the Command History Feature, page 2-7** (optional)

**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. These procedures are optional.

Beginning in privileged EXEC mode, enter this command to change the number of command lines that the switch records during the current terminal session:

```
Switch# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the switch records for all sessions on a particular line:

```
Switch(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

**Recalling Commands**

To recall commands from the history buffer, perform one of the actions listed in **Table 2-4**. These actions are optional.

<table>
<thead>
<tr>
<th><strong>Table 2-4</strong></th>
<th><strong>Recalling Commands</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td><strong>Result</strong></td>
</tr>
<tr>
<td>Press Ctrl-P or the up arrow key.</td>
<td>Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Press Ctrl-N or the down arrow key.</td>
<td>Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.</td>
</tr>
<tr>
<td>show history</td>
<td>While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that appear is controlled by the setting of the <code>terminal history</code> global configuration command and the <code>history</code> line configuration command.</td>
</tr>
</tbody>
</table>

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.
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. These procedures are optional.

To disable the feature during the current terminal session, enter the `terminal no history` privileged EXEC command.

To disable command history for the line, enter the `no history` line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line. It contains these sections:

- Enabling and Disabling Editing Features, page 2-7 (optional)
- Editing Commands through Keystrokes, page 2-8 (optional)
- Editing Command Lines that Wrap, page 2-9 (optional)

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it, re-enable it, or configure a specific line to have enhanced editing. These procedures are optional.

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
Switch (config-line)# no editing
```

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
Switch# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
Switch(config-line)# editing
```
Editing Commands through Keystrokes

Table 2-5 shows the keystrokes that you need to edit command lines. These keystrokes are optional.

Table 2-5  Editing Commands through Keystrokes

<table>
<thead>
<tr>
<th>Capability</th>
<th>Keystroke1</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move around the command line to make changes or corrections.</td>
<td>Press Ctrl-B, or press the left arrow key.</td>
<td>Move the cursor back one character.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-F, or press the right arrow key.</td>
<td>Move the cursor forward one character.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-A.</td>
<td>Move the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-E.</td>
<td>Move the cursor to the end of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Esc B.</td>
<td>Move the cursor back one word.</td>
</tr>
<tr>
<td></td>
<td>Press Esc F.</td>
<td>Move the cursor forward one word.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-T.</td>
<td>Transpose the character to the left of the cursor with the character located at the cursor.</td>
</tr>
<tr>
<td>Recall commands from the buffer and paste them in the command line. The switch provides a buffer with the last ten items that you deleted.</td>
<td>Press Ctrl-Y.</td>
<td>Recall the most recent entry in the buffer.</td>
</tr>
<tr>
<td>Delete entries if you make a mistake or change your mind.</td>
<td>Press the Delete or Backspace key.</td>
<td>Erase the character to the left of the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-D.</td>
<td>Delete the character at the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-K.</td>
<td>Delete all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-U or Ctrl-X.</td>
<td>Delete all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-W.</td>
<td>Delete the word to the left of the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Esc D.</td>
<td>Delete from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Capitalize or lowercase words or capitalize a set of letters.</td>
<td>Press Esc C.</td>
<td>Capitalize at the cursor.</td>
</tr>
<tr>
<td></td>
<td>Press Esc L.</td>
<td>Change the word at the cursor to lowercase.</td>
</tr>
<tr>
<td>Designate a particular keystroke as an executable command, perhaps as a shortcut.</td>
<td>Press Ctrl-V or Esc Q.</td>
<td></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.

In this example, the access-list global configuration command entry 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.

Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Switch(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0
Switch(config)# $ tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Switch(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45

After you complete the entry, press Ctrl-A to check the complete syntax before pressing the Return key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, 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. For information about recalling previous command entries, see the “Editing Commands through Keystrokes” section on page 2-8.
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.

To use this functionality, enter a show or more command followed by the pipe character (|), one of the keywords begin, include, or exclude, and an expression that you want to search for or filter out:

```
command | {begin | include | exclude} regular-expression
```

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.

This example shows how to include in the output display only lines where the expression `protocol` appears:

```
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

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

Accessing the CLI through a Console Connection or through Telnet

Before you can access the CLI, you must connect a terminal or PC to the switch console port and power on the switch, as described in the getting started guide that shipped with your switch. Then, to understand the boot process and the options available for assigning IP information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway.”

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. For more information, see the “Setting a Telnet Password for a Terminal Line” section on page 8-6.

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

- Connect the switch console port to a management station or dial-up modem. For information about connecting to the console port, see the switch getting started guide or 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.

For information about configuring the switch for Telnet access, see the “Setting a Telnet Password for a Terminal Line” section on page 8-6. The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

For information about configuring the switch for SSH, see the “Configuring the Switch for Secure Shell” section on page 8-45. The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.
Assigning the Switch IP Address and Default Gateway

This chapter describes how to create the initial switch configuration (for example, assigning the IP address and default gateway information) for the Catalyst 3560 switch by using a variety of automatic and manual methods. It also describes how to modify the switch startup configuration.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Understanding the Boot Process, page 3-2
- Assigning Switch Information, page 3-3
- Checking and Saving the Running Configuration, page 3-16
- Modifying the Startup Configuration, page 3-18
- Scheduling a Reload of the Software Image, page 3-23

Information in this chapter about configuring IP addresses and DHCP is specific to IP Version 4 (IPv4). If you plan to enable IP Version 6 (IPv6) forwarding on your switch, see Chapter 38, “Configuring IPv6 Unicast Routing” for information specific to IPv6 address format and configuration. To enable IPv6, the switch must be running the IP services image.
Understanding the 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 for setting up the initial switch configuration (IP address, subnet mask, default gateway, secret and Telnet passwords, and so forth).

The normal boot process involves the operation of the boot loader software, which performs these activities:

- 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. It tests the CPU DRAM and the portion of the flash device that makes up the flash file system.
- Loads a default operating system software image into memory and boots up the switch.

The boot loader provides access to the flash file system before the operating system is loaded. Normally, the boot loader is used only to load, uncompress, and launch 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 mechanism 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. For more information, see the “Recovering from a Software Failure” section on page 48-2 and the “Recovering from a Lost or Forgotten Password” section on page 48-3.

Note

You can disable password recovery. For more information, see the “Disabling Password Recovery” section on page 8-5.

Before you can assign switch information, make sure you have connected a PC or terminal to the console port, and configured the PC or terminal-emulation software baud rate and character format to match these of the switch console port:

- 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 1.
- Parity settings default is none.
Assigning Switch Information

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. For more information about the setup program, see the hardware installation guide.

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 previously.

- Default Switch Information, page 3-3
- Understanding DHCP-Based Autoconfiguration, page 3-3
- Manually Assigning IP Information, page 3-15

Default Switch Information

Table 3-1 shows the 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 <em>Switch</em>.</td>
</tr>
<tr>
<td>Telnet password</td>
<td>No password is defined.</td>
</tr>
<tr>
<td>Cluster command switch functionality</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Cluster name</td>
<td>No cluster name is defined.</td>
</tr>
</tbody>
</table>

Understanding DHCP-Based Autoconfiguration

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 a mechanism 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 are using 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.

Figure 3-1 shows the sequence of messages that are exchanged between the DHCP client and the DHCP server.

**Figure 3-1 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. For more information, see the “Configuring the TFTP Server” section on page 3-8.

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 switch. However, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch broadcasts, instead of unicasts, TFTP requests to obtain the switch configuration file.

The DHCP hostname option allows a group of switches to obtain hostnames and a standard configuration from the central management DHCP server. A client (switch) includes in its DCHPDISCOVER message an option 12 field used to request a hostname and other configuration parameters from the DHCP server. The configuration files on all clients are identical except for their DHCP-obtained hostnames.

If a client has a default hostname (the `hostname name` global configuration command is not configured or the `no hostname` global configuration command is entered to remove the hostname), the DHCP hostname option is not included in the packet when you enter the `ip address dhcp` interface configuration command. In this case, if the client receives the DHCP hostname option from the DHCP interaction while acquiring an IP address for an interface, the client accepts the DHCP hostname option and sets the flag to show that the system now has a hostname configured.

### Understanding 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. This 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.

#### 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 file) settings.

For procedures to configure the switch as a DHCP server, see the “Configuring DHCP-Based Autoconfiguration” section on page 3-7 and the “Configuring DHCP” section of the “IP addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.2.

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.

Limitations and Restrictions

These are the limitations:

- 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 it 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. Note that if the downloaded configuration is saved to the startup configuration, the feature is not triggered during subsequent system restarts.
Configuring DHCP-Based Autoconfiguration

These sections contain this configuration information:

- DHCP Server Configuration Guidelines, page 3-7
- Configuring the TFTP Server, page 3-8
- Configuring the DNS, page 3-8
- Configuring the Relay Device, page 3-8
- Obtaining Configuration Files, page 3-9
- Example Configuration, page 3-10

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)
- Router IP address (default gateway address to be used by the switch) (required)
- DNS server IP address (optional)

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. If your DHCP server is a Cisco device, for additional information about configuring DHCP, see the “Configuring DHCP” section of the “IP Addressing and Services” section of the Cisco IOS IP Configuration Guide from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides.
Configuring the TFTP Server

Based on the DHCP server configuration, the switch attempts to download one or more configuration files from the TFTP server. If you configured the DHCP server to respond to the switch with all the options required for IP connectivity to the TFTP server, and if you configured the DHCP server with a TFTP server name, address, and configuration filename, the switch attempts to download the specified configuration file from the specified TFTP server.

If you did not specify the configuration filename, the TFTP server, or if the configuration file could not be downloaded, the switch attempts to download a configuration file by using various combinations of filenames and TFTP server addresses. The files include the specified configuration filename (if any) and these files: network-config, cisconet.cfg, hostname.config, or hostname.cfg, where hostname is the switch’s current hostname. The TFTP server addresses used include the specified TFTP server address (if any) and the broadcast address (255.255.255.255).

For the switch to successfully download a configuration file, the TFTP server must contain one or more configuration files in its base directory. The files can include these files:

- The configuration file named in the DHCP reply (the actual switch configuration file).
- The network-config or the cisconet.cfg file (known as the default configuration files).
- The router-config or the 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. For more information, see the “Configuring the Relay Device” section on page 3-8. The preferred solution is to configure the DHCP server with all the required information.

Configuring the DNS

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 or on a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a router.

Configuring the Relay Device

You must configure a relay device, also referred to as a relay agent, when a switch sends broadcast packets that require a response from a host on a different LAN. Examples of broadcast packets that the switch might send are DHCP, DNS, and in some cases, TFTP packets. You must configure this relay device to forward received broadcast packets on an interface to the destination host.

If the relay device is a Cisco router, enable IP routing (ip routing global configuration command), and configure helper addresses by using the ip helper-address interface configuration command.
For example, in Figure 3-2, configure the router interfaces as follows:

On interface 10.0.0.2:

```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

On interface 20.0.0.1:

```
router(config-if)# ip helper-address 10.0.0.1
```

Note: If the switch is acting as the relay device, configure the interface as a routed port. For more information, see the “Routed Ports” section on page 11-4 and the “Configuring Layer 3 Interfaces” section on page 11-25.

Figure 3-2 Relay Device Used in Autoconfiguration

Obtaining Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in these ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).
  
  The switch receives its IP address, subnet mask, TFTP server address, and the configuration filename from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server and upon receipt, it completes its boot-up process.

- The IP address and the configuration filename is reserved for the switch, but the TFTP server address is not provided in the DHCP reply (one-file read method).
  
  The switch receives its IP address, subnet mask, and the configuration filename from the DHCP server. The switch sends a broadcast message to a TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, it completes its boot-up process.
• Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

The switch receives its IP address, subnet mask, and the TFTP server address from the DHCP server. The switch sends a unicast message to the TFTP server to retrieve the network-config or cisconet.cfg default configuration file. (If the network-config file cannot be read, the switch reads the cisconet.cfg file.)

The default configuration file contains the hostnames-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its hostname. If the hostname is not found in the file, the switch uses the hostname in the DHCP reply. If the hostname is not specified in the DHCP reply, the switch uses the default Switch as its hostname.

After obtaining its hostname from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its hostname (hostname-config or hostname.cfg, depending on whether network-config or cisconet.cfg was read earlier) from the TFTP server. If the cisconet.cfg file is read, the filename of the host is truncated to eight characters.

If the switch cannot read the network-config, cisconet.cfg, or the hostname file, it reads the router-config file. If the switch cannot read the router-config file, it reads the ciscortr.cfg file.

Note

The switch broadcasts TFTP server requests if the TFTP server is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

Example Configuration

Figure 3-3 shows a sample network for retrieving IP information by using DHCP-based autoconfiguration.

![Diagram](image)

Table 3-2 shows the configuration of the reserved leases on the DHCP server.
DNS Server Configuration

The DNS server maps the TFTP server name `tftpserver` to IP address 10.0.0.3.

**TFTP Server Configuration (on UNIX)**

The TFTP server base directory is set to `/tftpserver/work/`. This directory contains the network-config file used in the two-file read method. This file contains the hostname to be assigned to the switch based on its IP address. The base directory also contains a configuration file for each switch (`switcha-config`, `switchb-config`, and so forth) as shown in this display:

```
prompt> cd /tftpserver/work/
prompt> ls
network-config
switcha-config
switchb-config
switchc-config
switchd-config

prompt> cat network-config
ip host switcha 10.0.0.21
ip host switchb 10.0.0.22
ip host switchc 10.0.0.23
ip host switchd 10.0.0.24
```

### DHCP Client Configuration

No configuration file is present on Switch A through Switch D.

**Configuration Explanation**

In Figure 3-3, Switch A reads its configuration file as follows:

- It obtains its IP address 10.0.0.21 from the DHCP server.
- If no configuration filename is given in the DHCP server reply, Switch A reads the network-config file from the base directory of the TFTP server.
- It adds the contents of the network-config file to its host table.
- It reads its host table by indexing its IP address 10.0.0.21 to its hostname (switcha).
- It reads the configuration file that corresponds to its hostname; for example, it reads `switch1-config` from the TFTP server.

Switches B through D retrieve their configuration files and IP addresses in the same way.

### Table 3-2 DHCP Server Configuration

<table>
<thead>
<tr>
<th></th>
<th>Switch A</th>
<th>Switch B</th>
<th>Switch C</th>
<th>Switch D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding key (hardware address)</td>
<td>00e0.9f1e.2001</td>
<td>00e0.9f1e.2002</td>
<td>00e0.9f1e.2003</td>
<td>00e0.9f1e.2004</td>
</tr>
<tr>
<td>IP address</td>
<td>10.0.0.21</td>
<td>10.0.0.22</td>
<td>10.0.0.23</td>
<td>10.0.0.24</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Router address</td>
<td>10.0.0.10</td>
<td>10.0.0.10</td>
<td>10.0.0.10</td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>DNS server address</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>TFTP server name</td>
<td>tftpserver or 10.0.0.3</td>
<td>tftpserver or 10.0.0.3</td>
<td>tftpserver or 10.0.0.3</td>
<td>tftpserver or 10.0.0.3</td>
</tr>
<tr>
<td>Boot filename</td>
<td>switcha-config</td>
<td>switchb-config</td>
<td>switchc-config</td>
<td>switchd-config</td>
</tr>
<tr>
<td>(configuration file)</td>
<td>(optional)</td>
<td>(optional)</td>
<td>(optional)</td>
<td>(optional)</td>
</tr>
<tr>
<td>Hostname (optional)</td>
<td>switcha</td>
<td>switchb</td>
<td>switchc</td>
<td>switchd</td>
</tr>
</tbody>
</table>
Configuring the DHCP Auto Configuration and Image Update Features

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. The client switch 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)

Beginning in privileged EXEC mode, follow these steps to configure DHCP autoconfiguration of the TFTP and DHCP settings on a new switch to download a new configuration file.

<table>
<thead>
<tr>
<th>Command</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> ip dhcp poolname</td>
<td>Create a name for the DHCP Server address pool, and enter DHCP pool configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> bootfile filename</td>
<td>Specify the name of the configuration file that is used as a boot image.</td>
</tr>
</tbody>
</table>
| **Step 4** network network-number mask prefix-length | Specify the subnet network number and mask of the DHCP address pool.  
  **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 | Specify the IP address of the default router for a DHCP client. |
| **Step 6** option 150 address | Specify the IP address of the TFTP server. |
| **Step 7** exit | Return to global configuration mode. |
| **Step 8** tftp-server flash:filename.text | Specify the configuration file on the TFTP server. |
| **Step 9** interface interface-id | Specify the address of the client that will receive the configuration file. |
| **Step 10** no switchport | Put the interface into Layer 3 mode. |
| **Step 11** ip address address mask | Specify the IP address and mask for the interface. |
| **Step 12** end | Return to privileged EXEC mode. |
| **Step 13** copy running-config startup-config | (Optional) Save your entries in the configuration file. |

This example shows how to configure a switch as a DHCP server so that it will download a configuration file:

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile 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 gigabitethernet0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```
Configuring DHCP Auto-Image Update (Configuration File and Image)

Beginning in privileged EXEC mode, follow these steps to configure DHCP autoconfiguration to configure TFTP and DHCP settings on a new switch to download a new image and a new configuration file.

**Note**
Before following the steps in this table, you must 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. This image must be a tar and not a bin file.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip dhcp pool name</td>
<td>Create a name for the DHCP server address pool and enter DHCP pool configuration mode.</td>
</tr>
<tr>
<td>Step 3 bootfile filename</td>
<td>Specify the name of the file that is used as a boot image.</td>
</tr>
<tr>
<td>Step 4 network network-number mask prefix-length</td>
<td>Specify the subnet network number and mask of the DHCP address pool. The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).</td>
</tr>
<tr>
<td>Step 5 default-router address</td>
<td>Specify the IP address of the default router for a DHCP client.</td>
</tr>
<tr>
<td>Step 6 option 150 address</td>
<td>Specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td>Step 7 option 125 hex</td>
<td>Specify the path to the text file that describes the path to the image file.</td>
</tr>
<tr>
<td>Step 8 copy tftp flash filename.txt</td>
<td>Upload the text file to the switch.</td>
</tr>
<tr>
<td>Step 9 copy tftp flash imagename.tar</td>
<td>Upload the tar file for the new image to the switch.</td>
</tr>
<tr>
<td>Step 10 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 11 tftp-server flash:config.text</td>
<td>Specify the Cisco IOS configuration file on the TFTP server.</td>
</tr>
<tr>
<td>Step 12 tftp-server flash:imagename.tar</td>
<td>Specify the image name on the TFTP server.</td>
</tr>
<tr>
<td>Step 13 tftp-server flash:filename.txt</td>
<td>Specify the text file that contains the name of the image file to download</td>
</tr>
<tr>
<td>Step 14 interface interface-id</td>
<td>Specify the address of the client that will receive the configuration file.</td>
</tr>
<tr>
<td>Step 15 no switchport</td>
<td>Put the interface into Layer 3 mode.</td>
</tr>
<tr>
<td>Step 16 ip address address mask</td>
<td>Specify the IP address and mask for the interface.</td>
</tr>
<tr>
<td>Step 17 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 18 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
This example shows how to configure a switch as a DHCP server so it downloads a configuration file:

```
Switch# config terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# default-router 10.10.10.1
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# option 125 hex 0000.0009.0879.6f69.6e73.7461.6c6c.5f686370
Switch(config)# tftp-server flash:config-boot.text
Switch(config)# tftp-server flash:c3560-ipservices-mz.122-44.3.SE.tar
Switch(config)# tftp-server flash:boot-config.text
Switch(config)# tftp-server flash: autoinstall_dhcp
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.10.10.1 255.255.255.0
Switch(config-if)# end
```

### Configuring the Client

Beginning in privileged EXEC mode, follow these steps to configure a switch to download a configuration file and new image from a DHCP server:

<table>
<thead>
<tr>
<th>Command</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>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>boot host dhcp</code></td>
<td>Enable autoconfiguration with a saved configuration.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>boot host retry timeout</code></td>
<td>(Optional) Set the amount of time the system tries to download a configuration file.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you do not set a timeout the system will indefinitely try to obtain an IP address from the DHCP server.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>banner config-save ^C warning-message ^C</code></td>
<td>(Optional) Create warning messages to be displayed when you try to save the configuration file to NVRAM.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>show boot</code></td>
<td>Verify the configuration.</td>
</tr>
</tbody>
</table>
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#
```

**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.

### Manually Assigning IP Information

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to multiple switched virtual interfaces (SVIs):

**Note**
If the switch is running the IP services image, you can also manually assign IP information to a port if you first put the port into Layer 3 mode by using the `no switchport` interface configuration command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface vlan vlan-id</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ip address ip-address subnet-mask</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. The VLAN range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>Enter the IP address and subnet mask.</td>
</tr>
<tr>
<td></td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>
Chapter 3      Assigning the Switch IP Address and Default Gateway

Checking and Saving the Running Configuration

You can check the configuration settings that you entered or changes that you made by entering this privileged EXEC command:

```
Switch# show running-config
Building configuration...

Current configuration: 1363 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch A
!
enable secret 5 $1$ej9.$DMUvAUnZOAmvmgqBEzIxE0
!
<output truncated>
.
interface gigabitethernet0/1
no switchport
ip address 172.20.137.50 255.255.255.0
!
interface gigabitethernet6/0/2
mvr type source
<output truncated>
.
```

To remove the switch IP address, use the **no ip address** interface configuration command. If you are removing the address through a Telnet session, your connection to the switch will be lost. To remove the default gateway address, use the **no ip default-gateway** global configuration command.

For information on setting the switch system name, protecting access to privileged EXEC commands, and setting time and calendar services, see Chapter 6, “Administering the Switch.”

### Checking and Saving the Running Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>ip default-gateway ip-address</strong> Enter 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. <strong>Note</strong> When your switch is configured to route with IP, it does not need to have a default gateway set.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>show interfaces vlan vlan-id</strong> Verify the configured IP address.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>show ip redirects</strong> Verify the configured default gateway.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>copy running-config startup-config</strong> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Step 5

```
ip default-gateway ip-address
```

Enter 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.

**Note** When your switch is configured to route with IP, it does not need to have a default gateway set.

Step 6

```
end
```

Return to privileged EXEC mode.

Step 7

```
show interfaces vlan vlan-id
```

Verify the configured IP address.

Step 8

```
show ip redirects
```

Verify the configured default gateway.

Step 9

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

(Optional) Save your entries in the configuration file.
interface VLAN1
  ip address 172.20.137.50 255.255.255.0
  no ip directed-broadcast
  !
  ip default-gateway 172.20.137.1 !
  !
  snmp-server community private RW
  snmp-server community public RO
  snmp-server community private@es0 RW
  snmp-server community public@es0 RO
  snmp-server chassis-id 0x12
  !
end

To store the configuration or changes you have made to your startup configuration in flash memory, enter this privileged EXEC command:

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

This command saves the configuration settings that you made. If you fail to do this, your configuration will be lost the next time you reload the system. To display information stored in the NVRAM section of flash memory, use the `show startup-config` or `more startup-config` privileged EXEC command.

For more information about alternative locations from which to copy the configuration file, see Appendix B, “Working with the Cisco IOS File System, Configuration Files, and Software Images.”

### 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. Typically, this occurs when you have many switches in a switch stack. You can configure the size of the NVRAM buffer to support larger configuration files. The new NVRAM buffer size is synced to all current and new member switches.

#### Note

After you configure the NVRAM buffer size, reload the switch or switch stack.

When you add a switch to a stack and the NVRAM size differs, the new switch syncs with the stack and reloads automatically.

Beginning in privileged EXEC mode, follow these steps to configure the NVRAM buffer size:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>boot buffersize size</td>
<td>Configure the NVRAM buffersize in KB. The valid range for <code>size</code> is from 4096 to 1048576.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show boot</td>
<td>Verify the configuration.</td>
</tr>
</tbody>
</table>
This example shows how to configure the NVRAM buffer size:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# boot buffersize 524288
Switch(config)# end
Switch# show boot
BOOT path-list:
Config file: flash:/config.text
Private Config file: flash:/private-config.text
Enable Break: no
Manual Boot: no
HELPER path-list:
Auto upgrade: yes
Auto upgrade path:
NVRAM/Config file
  buffer size: 524288
Timeout for Config
  Download: 300 seconds
Config Download
  via DHCP: enabled (next boot: enabled)
Switch#

Modifying the Startup Configuration

These sections describe how to modify the switch startup configuration:

- Default Boot Configuration, page 3-19
- Automatically Downloading a Configuration File, page 3-19
- Booting Manually, page 3-20
- Booting a Specific Software Image, page 3-21
- Controlling Environment Variables, page 3-22

See also Appendix B, “Working with the Cisco IOS File System, Configuration Files, and Software Images,” for information about switch configuration files.
Default Boot Configuration

Table 3-3 shows the default boot-up configuration.

Table 3-3  Default Boot Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system software image</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The switch attempts to automatically boot up the system using information in the BOOT environment variable. If the variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. The Cisco IOS image is stored in a directory that has the same name as the image file (excluding the .bin extension). In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.</td>
</tr>
<tr>
<td>Configuration file</td>
<td>Configured switches use the config.text file stored on the system board in flash memory. A new switch has no configuration file.</td>
</tr>
</tbody>
</table>

Automatically Downloading a Configuration File

You can automatically download a configuration file to your switch by using the DHCP-based autoconfiguration feature. For more information, see the “Understanding DHCP-Based Autoconfiguration” section on page 3-3.

Specifying the Filename to Read and Write the System Configuration

By default, the Cisco IOS software uses the file config.text 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-up cycle.

Beginning in privileged EXEC mode, follow these steps to specify a different configuration filename:

Command | Purpose
--------|-----------------|
**Step 1** configure terminal | Enter global configuration mode.
**Step 2** boot config-file flash:/file-url | Specify the configuration file to load during the next boot-up cycle. For file-url, specify the path (directory) and the configuration filename. Filenames and directory names are case sensitive.
**Step 3** end | Return to privileged EXEC mode.
**Step 4** show boot | Verify your entries. The boot config-file global configuration command changes the setting of the CONFIG_FILE environment variable.
**Step 5** copy running-config startup-config | (Optional) Save your entries in the configuration file.
To return to the default setting, use the `no boot config-file` global configuration command.

## Booting Manually

By default, the switch automatically boots up; however, you can configure it to manually boot up.

Beginning in privileged EXEC mode, follow these steps to configure the switch to manually boot up during the next boot cycle:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>boot manual</strong></td>
</tr>
<tr>
<td></td>
<td>Enable the switch to manually boot up during the next boot cycle.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>show boot</strong></td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>The <code>boot manual</code> global command changes the setting of the MANUAL_BOOT environment variable.</td>
</tr>
<tr>
<td></td>
<td>The next time you reboot the system, the switch is in boot loader mode, shown by the <code>switch:</code> prompt. To boot up the system, use the <code>boot filesystem:file-url</code> boot loader command.</td>
</tr>
<tr>
<td></td>
<td>• For filesystem:, use <code>flash:</code> for the system board flash device.</td>
</tr>
<tr>
<td></td>
<td>• For file-url, specify the path (directory) and the name of the bootable image.</td>
</tr>
<tr>
<td></td>
<td>Filenames and directory names are case sensitive.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>copy running-config startup-config</strong> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable manual booting, use the `no boot manual` global configuration command.
Booting a Specific Software Image

By default, the switch attempts to automatically boot up the system using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. However, you can specify a specific image to boot up.

Beginning in privileged EXEC mode, follow these steps to configure the switch to boot a specific image during the next boot cycle:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: boot system filesystem:file-url</td>
<td>Configure the switch to boot a specific image in flash memory during the next boot cycle.</td>
</tr>
<tr>
<td></td>
<td>• For filesystem:, use flash: for the system board flash device.</td>
</tr>
<tr>
<td></td>
<td>• For file-url, specify the path (directory) and the name of the bootable image.</td>
</tr>
<tr>
<td></td>
<td>Filenames and directory names are case sensitive.</td>
</tr>
<tr>
<td>Step 3: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4: show boot</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>The boot system global command changes the setting of the BOOT environment variable.</td>
</tr>
<tr>
<td></td>
<td>During the next boot cycle, the switch attempts to automatically boot up the system using information in the BOOT environment variable.</td>
</tr>
<tr>
<td>Step 5: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no boot system global configuration command.
Controlling Environment Variables

With a normally operating switch, you enter the boot loader mode only through a switch console connection configured for 9600 b/s. Unplug the switch power cord, and press the switch Mode button while reconnecting the power cord. You can release the Mode button a second or two after the LED above port 1 turns off. Then the boot loader switch: prompt appears.

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, behaves. 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 listed in this file; it has a value if it is listed in the file 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.

Note

For complete syntax and usage information for the boot loader commands and environment variables, see the command reference for this release.
Table 3-4 describes the function of the most common environment variables.

Table 3-4 Environment Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Boot Loader Command</th>
<th>Cisco IOS Global Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT</td>
<td>set BOOT filesystem:file-url ...</td>
<td>boot system filesystem:file-url ...</td>
</tr>
<tr>
<td></td>
<td>A semicolon-separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.</td>
<td>Specifies the Cisco IOS image to load during the next boot cycle. This command changes the setting of the BOOT environment variable.</td>
</tr>
<tr>
<td>MANUAL_BOOT</td>
<td>set MANUAL_BOOT yes</td>
<td>boot manual</td>
</tr>
<tr>
<td></td>
<td>Decides whether the switch automatically or manually boots up. Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the boot loader mode.</td>
<td>Enables manually booting up the switch during the next boot cycle and changes the setting of the MANUAL_BOOT environment variable. The next time you reboot the system, the switch is in boot loader mode. To boot up the system, use the boot flash:filesystem:file-url boot loader command, and specify the name of the bootable image.</td>
</tr>
<tr>
<td>CONFIG_FILE</td>
<td>set CONFIG_FILE flash:file-url</td>
<td>boot config-file flash:file-url</td>
</tr>
<tr>
<td></td>
<td>Changes the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</td>
<td>Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. This command changes the CONFIG_FILE environment variable.</td>
</tr>
</tbody>
</table>

**Scheduling a 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.
Configuring a Scheduled Reload

To configure your switch to reload the software image at a later time, use one of these commands in privileged EXEC mode:

- **`reload in [hh:]mm [text]`**
  
  This command 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.

- **`reload at hh:mm [month day | day month] [text]`**
  
  This command schedules a 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.

  **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.

The `reload` command halts the system. If the system is not set to manually boot up, it reboots itself. Use the `reload` command after you save the switch configuration information to the startup configuration (`copy running-config startup-config`).

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 thereby 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.

This example shows how to reload the software on the switch on the current day at 7:30 p.m:

```bash
Switch# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 1996 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

This example shows how to reload the software on the switch at a future time:

```bash
Switch# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 1996 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

To cancel a previously scheduled reload, use the `reload cancel` privileged EXEC command.
Displaying Scheduled Reload Information

To display information about a previously scheduled reload or to find out if a reload has been scheduled on the switch, use the show reload privileged EXEC command.

It displays reload information including the time the reload is scheduled to occur and the reason for the reload (if it was specified when the reload was scheduled).
Configuring Cisco IOS Configuration Engine

This chapter describes how to configure the feature on the Catalyst 3560 switch.

**Note**


- Understanding Cisco Configuration Engine Software, page 4-1
- Understanding Cisco IOS Agents, page 4-5
- Configuring Cisco IOS Agents, page 4-6
- Displaying CNS Configuration, page 4-13

**Understanding Cisco Configuration Engine Software**

The Cisco Configuration Engine is network management software that acts as a configuration service for automating the deployment and management of network devices and services (see Figure 4-1). Each 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 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 Configuration Engine supports standalone and server modes and has these CNS components:

- Configuration service (web server, file manager, and namespace mapping server)
- Event service (event gateway)
- Data service directory (data models and schema)

In standalone mode, the Configuration Engine supports an embedded Directory Service. In this mode, no external directory or other data store is required. In server mode, the Configuration Engine supports the use of a user-defined external directory.
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 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 agent is on the switch and facilitates the communication between the switch and the event gateway on the 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 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.

What You Should Know About the CNS IDs and Device Hostnames

The 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 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.

Because the Configuration Engine 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.

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.

ConfigID

Each configured switch has a unique ConfigID, which serves as the key into the 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 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. All switches configured with the `cns config partial` global configuration command must access the event bus. Therefore, the DeviceID, as originated on the switch, must match the DeviceID of the corresponding switch definition in the Configuration Engine.

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 caches 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. Enter the `no cns event` global configuration command followed by the `cns event` global configuration command.

When the connection is re-established, the switch sends its modified hostname to the event gateway. The event gateway redefines the DeviceID to the new value.

Caution

When using the Configuration Engine user interface, you must first set the DeviceID field to the hostname value that the switch acquires after—not before—you use the `cns config initial` global configuration command at the switch. Otherwise, subsequent `cns config partial` global configuration command operations malfunction.

Using 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 Configuration Engine.

Note

For more information about running the setup program on the Configuration Engine, see the Configuration Engine setup and configuration guide:

Understanding Cisco IOS Agents

The CNS event agent feature allows the switch to publish and subscribe to events on the event bus and works with the Cisco IOS agent. The Cisco IOS agent feature supports the switch by providing these features:

- Initial Configuration, page 4-5
- Incremental (Partial) Configuration, page 4-6
- Synchronized Configuration, page 4-6

Initial Configuration

When the switch first comes up, it attempts to get an IP address by broadcasting a DHCP request on the network. Assuming there is no DHCP server on the subnet, the distribution switch acts as a DHCP relay agent and forwards the request to the DHCP server. Upon receiving the request, the DHCP server assigns an IP address to the new switch and includes the TFTP server IP address, the path to the bootstrap configuration file, and the default gateway IP address in a unicast reply to the DHCP relay agent. The DHCP relay agent forwards the reply to the switch.

The switch automatically configures the assigned IP address on interface VLAN 1 (the default) and downloads the bootstrap configuration file from the TFTP server. Upon successful download of the bootstrap configuration file, the switch loads the file in its running configuration.

The Cisco IOS agents initiate communication with the Configuration Engine by using the appropriate ConfigID and EventID. The Configuration Engine maps the Config ID to a template and downloads the full configuration file to the switch.

Figure 4-2 shows a sample network configuration for retrieving the initial bootstrap configuration file by using DHCP-based autoconfiguration.

Figure 4-2  Initial Configuration Overview
Incremental (Partial) Configuration

After the network is running, new services can be added by using the Cisco IOS agent. Incremental (partial) configurations can be sent to the switch. The actual configuration can be sent as an event payload by way of the event gateway (push operation) or as a signal event that triggers the switch to initiate a pull operation.

The switch can check the syntax of the configuration before applying it. If the syntax is correct, the switch applies the incremental configuration and publishes an event that signals success to the configuration server. If the switch does not apply the incremental configuration, it publishes an event showing an error status. When the switch has applied the incremental configuration, it can write it to NVRAM or wait until signaled to do so.

Synchronized Configuration

When the switch receives a configuration, it can defer application of the configuration upon receipt of a write-signal event. The write-signal event tells the switch not to save the updated configuration into its NVRAM. The switch uses the updated configuration as its running configuration. This ensures that the switch configuration is synchronized with other network activities before saving the configuration in NVRAM for use at the next reboot.

Configuring Cisco IOS Agents

The Cisco IOS agents embedded in the switch Cisco IOS software allow the switch to be connected and automatically configured as described in the “Enabling Automated CNS Configuration” section on page 4-6. If you want to change the configuration or install a custom configuration, see these sections for instructions:

- Enabling the CNS Event Agent, page 4-7
- Enabling the Cisco IOS CNS Agent, page 4-9

Enabling Automated CNS Configuration

To enable automated CNS configuration of the switch, you must first complete the prerequisites in Table 4-1. When you complete them, power on the switch. At the setup prompt, do nothing: The switch begins the initial configuration as described in the “Initial Configuration” section on page 4-5. When the full configuration file is loaded on your switch, you need to do nothing else.

<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>
</tbody>
</table>
Table 4-1  Prerequisites for Enabling Automatic Configuration (continued)

<table>
<thead>
<tr>
<th>Device</th>
<th>Required Configuration</th>
</tr>
</thead>
</table>
| DHCP server             | • IP address assignment  
                          | • TFTP server IP address  
                          | • Path to bootstrap configuration file on the TFTP server  
                          | • Default gateway IP address                                                   |
| TFTP server             | • A bootstrap configuration file that includes the CNS configuration commands that enable the switch to communicate with the Configuration Engine  
                          | • 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  
                          | • The CNS event agent configured to push the configuration file to the switch |
| CNS Configuration Engine| One or more templates for each type of device, with the ConfigID of the device mapped to the template. |

Note: For more information about running the setup program and creating templates on the Configuration Engine, see the Cisco Configuration Engine Installation and Setup Guide, 1.5 for Linux: http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/1.5/installation_linux/guide/setup_1.html

Enabling the CNS Event Agent

Note: You must enable the CNS event agent on the switch before you enable the CNS configuration agent.
Beginning in privileged EXEC mode, follow these steps to enable the CNS event agent on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>cns event {hostname</td>
</tr>
<tr>
<td></td>
<td>Enable the event agent, and enter the gateway parameters.</td>
</tr>
<tr>
<td></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) Enter backup to show that this is the backup gateway. (If omitted, this is the primary gateway.)</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 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 reconnect 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) For source ip-address, enter the source IP address of this device.</td>
</tr>
<tr>
<td></td>
<td>Note Though visible in the command-line help string, the encrypt and the clock-timeout time keywords are not supported.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show cns event connections</td>
</tr>
<tr>
<td></td>
<td>Verify information about the event agent.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the CNS event agent, use the no cns event {ip-address | hostname} global configuration command.

This example shows how to enable the CNS event agent, set the IP address gateway to 10.180.1.27, set 120 seconds as the keepalive interval, and set 10 as the retry count.

Switch(config)# cns event 10.180.1.27 keepalive 120 10
After enabling the CNS event agent, start the Cisco IOS CNS agent on the switch. You can enable the Cisco IOS agent with these commands:

- The `cns config initial` global configuration command enables the Cisco IOS agent and initiates an initial configuration on the switch.
- The `cns config partial` global configuration command enables the Cisco IOS agent and initiates a partial configuration on the switch. You can then use the Configuration Engine to remotely send incremental configurations to the switch.

### Enabling an Initial Configuration

Beginning in privileged EXEC mode, follow these steps to enable the CNS configuration agent and initiate an initial configuration on the switch:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>cns template connect name</code></td>
<td>Enter CNS template connect configuration mode, and specify the name of the CNS connect template.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>cli config-text</code></td>
<td>Enter a command line for the CNS connect template. Repeat this step for each command line in the template.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
<td>Repeat Steps 2 to 3 to configure another CNS connect template.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 6 | `cns connect name [retries number] [retry-interval seconds] [sleep seconds] [timeout seconds]` | Enter CNS connect configuration mode, specify the name of the CNS connect profile, and define the profile parameters. The switch uses the CNS connect profile to connect to the Configuration Engine.  
  - (Optional) For `retries number`, enter the number of connection retries. The range is 1 to 30. The default is 3.  
  - (Optional) For `retry-interval seconds`, enter the interval between successive connection attempts to the Configuration Engine. The range is 1 to 40 seconds. The default is 10 seconds.  
  - (Optional) For `sleep seconds`, enter the amount of time before which the first connection attempt occurs. The range is 0 to 250 seconds. The default is 0.  
  - (Optional) For `timeout seconds`, enter the amount of time after which the connection attempts end. The range is 10 to 2000 seconds. The default is 120. |
Step 7  
```
discover {controller controller-type | dlc
 [subinterface subinterface-number] | interface
 [interface-type] | line line-type}
```
Specify the interface parameters in the CNS connect profile.
- For `controller controller-type`, enter the controller type.
- For `dlci`, enter the active data-link connection identifiers (DLCIs).
  (Optional) For `subinterface subinterface-number`, specify the point-to-point subinterface number that is used to search for active DLCIs.
- For `interface [interface-type]`, enter the type of interface.
- For `line line-type`, enter the line type.

Step 8  
```
template name [ ... name]
```
Specify the list of CNS connect templates in the CNS connect profile to be applied to the switch configuration. You can specify more than one template.

Step 9  
```
extit
```
Return to global configuration mode.

Step 10  
```
hostname name
```
Enter the hostname for the switch.

Step 11  
```
ip route network-number
```
(Optional) Establish a static route to the Configuration Engine whose IP address is `network-number`.

Step 12  
```
cns id interface num | dns-reverse | ipaddress
 | mac-address | [event] [image]
```
(Optional) Set the unique EventID or ConfigID used by the Configuration Engine.
- For `interface num`, enter the type of interface—for example, ethernet, group-async, loopback, or virtual-template. This setting specifies from which interface the IP or MAC address should be retrieved to define the unique ID.
- For `{ dns-reverse | ipaddress | mac-address }`, enter `dns-reverse` to retrieve the hostname and assign it as the unique ID, enter `ipaddress` to use the IP address, or enter `mac-address` to use the MAC address as the unique ID.
- (Optional) Enter `event` to set the ID to be the event-id value used to identify the switch.
- (Optional) Enter `image` to set the ID to be the image-id value used to identify the switch.

Note  
If both the `event` and `image` keywords are omitted, the image-id value is used to identify the switch.
- For `{ hardware-serial | hostname | string string | udi }`, enter `hardware-serial` to set the switch serial number as the unique ID, enter `hostname` (the default) to select the switch hostname as the unique ID, enter an arbitrary text string for `string string` as the unique ID, or enter `udi` to set the unique device identifier (UDI) as the unique ID.
Step 14

\texttt{cns \_config \_initial \{hostname | ip-address\} [port-number] [event] [no-persist] [page page] [source ip-address] [syntax-check]}

Enable the Cisco IOS agent, and initiate an initial configuration.

- For \{hostname | ip-address\}, enter the hostname or the IP address of the configuration server.
- (Optional) For \texttt{port-number}, enter the port number of the configuration server. The default port number is 80.
- (Optional) Enable \texttt{event} for configuration success, failure, or warning messages when the configuration is finished.
- (Optional) Enable \texttt{no-persist} to suppress the automatic writing to NVRAM of the configuration pulled as a result of entering the \texttt{cns \_config \_initial} global configuration command. If the \texttt{no-persist} keyword is not entered, using the \texttt{cns \_config \_initial} command causes the resultant configuration to be automatically written to NVRAM.
- (Optional) For \texttt{page page}, enter the web page of the initial configuration. The default is /Config/config/asp.
- (Optional) Enter \texttt{source ip-address} to use for source IP address.
- (Optional) Enable \texttt{syntax-check} to check the syntax when this parameter is entered.

Note Though visible in the command-line help string, the \texttt{encrypt}, \texttt{status url}, and \texttt{inventory} keywords are not supported.

Step 15
\texttt{end} 
Return to privileged EXEC mode.

Step 16
\texttt{show cns \_config \_connections} 
Verify information about the configuration agent.

Step 17
\texttt{show \_running-\_config} 
Verify your entries.

To disable the CNS Cisco IOS agent, use the \texttt{no cns config initial \{ip-address | hostname\}} global configuration command.

This example shows how to configure an initial configuration on a remote switch when the switch configuration is unknown (the CNS Zero Touch feature).

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 $(next-hop)
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# cns config initial 10.1.1.1 no-persist
```
This example shows how to configure an initial configuration on a remote switch when the switch IP address is known. The Configuration Engine IP address is 172.28.129.22.

```
Switch(config)# cns template connect template-dhcp
Switch(config-tmpl-conn)# cli ip address dhcp
Switch(config-tmpl-conn)# exit
Switch(config)# cns template connect template-ip-route
Switch(config-tmpl-conn)# cli ip route 0.0.0.0 0.0.0.0 $next-hop
Switch(config-tmpl-conn)# exit
Switch(config)# cns connect dhcp
Switch(config-cns-conn)# discover interface gigabitethernet
Switch(config-cns-conn)# template template-dhcp
Switch(config-cns-conn)# template ip-route
Switch(config-cns-conn)# exit
Switch(config)# hostname RemoteSwitch
RemoteSwitch(config)# ip route 172.28.129.22 255.255.255.255 11.11.11.1
RemoteSwitch(config)# cns id ethernet 0 ipaddress
RemoteSwitch(config)# cns config initial 172.28.129.22 no-persist
```

### Enabling a Partial Configuration

Beginning in privileged EXEC mode, follow these steps to enable the Cisco IOS agent and to initiate a partial configuration on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>cns config partial {ip-address</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show cns config stats or show cns config outstanding</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable the Cisco IOS agent, use the no cns config partial {ip-address | hostname} global configuration command. To cancel a partial configuration, use the cns config cancel privileged EXEC command.
Displaying CNS Configuration

Table 4-2 Privileged EXEC show Commands

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

This chapter provides the concepts and procedures to create and manage Catalyst 3560 switch clusters. You can create and manage switch clusters by using Cisco Network Assistant (hereafter known as Network Assistant), the command-line interface (CLI), or SNMP. For complete procedures, see the online help. For the CLI cluster commands, see the switch command reference.

Note

Network Assistant supports switch clusters, but we recommend that you instead group switches into communities. Network Assistant has a Cluster Conversion Wizard to help you convert a cluster to a community. For more information about Network Assistant, including introductory information on managing switch clusters and converting a switch cluster to a community, see Getting Started with Cisco Network Assistant, available on Cisco.com.

This chapter focuses on Catalyst 3560 switch clusters. It also includes guidelines and limitations for clusters mixed with other cluster-capable Catalyst switches, but it does not provide complete descriptions of the cluster features for these other switches. For complete cluster information for a specific Catalyst platform, refer to the software configuration guide for that switch.

This chapter consists of these sections:

- Understanding Switch Clusters, page 5-1
- Planning a Switch Cluster, page 5-5
- Using the CLI to Manage Switch Clusters, page 5-16
- Using SNMP to Manage Switch Clusters, page 5-16

Note

We do not recommend using the `ip http access-class` global configuration command to limit access to specific hosts or networks. Access should be controlled through the cluster command switch or by applying access control lists (ACLs) on interfaces that are configured with IP address. For more information on ACLs, see Chapter 33, “Configuring Network Security with ACLs.”

Understanding Switch Clusters

A switch cluster is a set of up to 16 connected, cluster-capable Catalyst switches that are managed as a single entity. The switches in the cluster use the switch clustering technology so that you can configure and troubleshoot a group of different Catalyst desktop switch platforms through a single IP address.
In a switch cluster, 1 switch must be the cluster command switch and up to 15 other switches can be cluster member switches. The total number of switches in a cluster cannot exceed 16 switches. The cluster command switch is the single point of access used to configure, manage, and monitor the cluster member switches. Cluster members can belong to only one cluster at a time.

The benefits of clustering switches include:

- Management of Catalyst switches regardless of their interconnection media and their physical locations. The switches can be in the same location, or they can be distributed across a Layer 2 or Layer 3 (if your cluster is using a Catalyst 3550, Catalyst 3560, or Catalyst 3750 switch as a Layer 3 router between the Layer 2 switches in the cluster) network.

Cluster members are connected to the cluster command switch according to the connectivity guidelines described in the “Automatic Discovery of Cluster Candidates and Members” section on page 5-5. This section includes management VLAN considerations for the Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches. For complete information about these switches in a switch-cluster environment, refer to the software configuration guide for that specific switch.

- Command-switch redundancy if a cluster command switch fails. One or more switches can be designated as standby cluster command switches to avoid loss of contact with cluster members. A cluster standby group is a group of standby cluster command switches.

- Management of a variety of Catalyst switches through a single IP address. This conserves on IP addresses, especially if you have a limited number of them. All communication with the switch cluster is through the cluster command switch IP address.

Table 5-1 lists the Catalyst switches eligible for switch clustering, including which ones can be cluster command switches and which ones can only be cluster member switches, and the required software versions.

**Table 5-1 Switch Software and Cluster Capability**

<table>
<thead>
<tr>
<th>Switch</th>
<th>Cisco IOS Release</th>
<th>Cluster Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3750-X or Catalyst 3560-X</td>
<td>12.2(53)SE2 or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 3750-E or Catalyst 3560-E</td>
<td>12.2(35)SE2 or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 3750</td>
<td>12.1(11)AX or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 3560</td>
<td>12.1(19)EA1b or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 3550</td>
<td>12.1(4)EA1 or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2975</td>
<td>12.2(46)EX or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2970</td>
<td>12.1(11)AX or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2960-S</td>
<td>12.2(53)SE or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2960</td>
<td>12.2(25)FX or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2955</td>
<td>12.1(12c)EA1 or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2950</td>
<td>12.0(5.2)WC(1) or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2950 LRE</td>
<td>12.1(11)Y or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2940</td>
<td>12.1(13)AY or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 3500 XL</td>
<td>12.0(5.1)XU or later</td>
<td>Member or command switch</td>
</tr>
<tr>
<td>Catalyst 2900 XL (8-MB switches)</td>
<td>12.0(5.1)XU or later</td>
<td>Member or command switch</td>
</tr>
</tbody>
</table>
Cluster Command Switch Characteristics

A cluster command switch must meet these requirements:

- It is running Cisco IOS Release 12.1(19)EA1 or later.
- It has an IP address.
- It has Cisco Discovery Protocol (CDP) version 2 enabled (the default).
- It is not a command or cluster member switch of another cluster.
- It is connected to the standby cluster command switches through the management VLAN and to the cluster member switches through a common VLAN.

Standby Cluster Command Switch Characteristics

A standby cluster command switch must meet these requirements:

- It is running Cisco IOS 12.1(19)EA1 or later.
- It has an IP address.
- It has CDP version 2 enabled.
- It is connected to the command switch and to other standby command switches through its management VLAN.
- It is connected to all other cluster member switches (except the cluster command and standby command switches) through a common VLAN.
- It is redundantly connected to the cluster so that connectivity to cluster member switches is maintained.
- It is not a command or member switch of another cluster.

Note

Standby cluster command switches must be the same type of switches as the cluster command switch. For example, if the cluster command switch is a Catalyst 3560 switch, the standby cluster command switches must also be Catalyst 3560 switches. Refer to the switch configuration guide of other cluster-capable switches for their requirements on standby cluster command switches.

Candidate Switch and Cluster Member Switch Characteristics

Candidate switches are cluster-capable switches that have not yet been added to a cluster. Cluster member switches are switches that have actually been added to a switch cluster. Although not required, a candidate or cluster member switch can have its own IP address and password (for related considerations, see the “IP Addresses” section on page 5-14 and “Passwords” section on page 5-14).
To join a cluster, a candidate switch must meet these requirements:

- It is running cluster-capable software.
- It has CDP version 2 enabled.
- It is not a command or cluster member switch of another cluster.
- If a cluster standby group exists, it is connected to every standby cluster command switch through at least one common VLAN. The VLAN to each standby cluster command switch can be different.
- It is connected to the cluster command switch through at least one common VLAN.

**Note**

Catalyst 1900, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL candidate and cluster member switches must be connected through their management VLAN to the cluster command switch and standby cluster command switches. For complete information about these switches in a switch-cluster environment, refer to the software configuration guide for that specific switch.

This requirement does not apply if you have a Catalyst 2970, Catalyst 3550, Catalyst 3560, or Catalyst 3750 cluster command switch. Candidate and cluster member switches can connect through any VLAN in common with the cluster command switch.
Anticipating conflicts and compatibility issues is a high priority when you manage several switches through a cluster. This section describes these guidelines, requirements, and caveats that you should understand before you create the cluster:

- Automatic Discovery of Cluster Candidates and Members, page 5-5
- HSRP and Standby Cluster Command Switches, page 5-11
- IP Addresses, page 5-14
- Hostnames, page 5-14
- Passwords, page 5-14
- SNMP Community Strings, page 5-15
- TACACS+ and RADIUS, page 5-15
- LRE Profiles, page 5-15

Refer to the release notes for the list of Catalyst switches eligible for switch clustering, including which ones can be cluster command switches and which ones can only be cluster member switches, and for the required software versions and browser and Java plug-in configurations.

### Automatic Discovery of Cluster Candidates and Members

The cluster command switch uses Cisco Discovery Protocol (CDP) to discover cluster member switches, candidate switches, neighboring switch clusters, and edge devices across multiple VLANs and in star or cascaded topologies.

**Note**

Do not disable CDP on the cluster command switch, on cluster members, or on any cluster-capable switches that you might want a cluster command switch to discover. For more information about CDP, see Chapter 24, “Configuring CDP.”

Following these connectivity guidelines ensures automatic discovery of the switch cluster, cluster candidates, connected switch clusters, and neighboring edge devices:

- Discovery Through CDP Hops, page 5-5
- Discovery Through Non-CDP-Capable and Noncluster-Capable Devices, page 5-7
- Discovery Through Different VLANs, page 5-7
- Discovery Through Different Management VLANs, page 5-8
- Discovery Through Routed Ports, page 5-9
- Discovery of Newly Installed Switches, page 5-10

### Discovery Through CDP Hops

By using CDP, a cluster command switch can discover switches up to seven CDP hops away (the default is three hops) from the edge of the cluster. The edge of the cluster is where the last cluster member switches are connected to the cluster and to candidate switches. For example, cluster member switches 9 and 10 in Figure 5-1 are at the edge of the cluster.
In Figure 5-1, the cluster command switch has ports assigned to VLANs 16 and 62. The CDP hop count is three. The cluster command switch discovers switches 11, 12, 13, and 14 because they are within three hops from the edge of the cluster. It does not discover switch 15 because it is four hops from the edge of the cluster.

**Figure 5-1 Discovery Through CDP Hops**
Discovery Through Non-CDP-Capable and Noncluster-Capable Devices

If a cluster command switch is connected to a *non-CDP-capable third-party hub* (such as a non-Cisco hub), it can discover cluster-enabled devices connected to that third-party hub. However, if the cluster command switch is connected to a *noncluster-capable Cisco device*, it cannot discover a cluster-enabled device connected beyond the noncluster-capable Cisco device.

*Figure 5-2* shows that the cluster command switch discovers the switch that is connected to a third-party hub. However, the cluster command switch does not discover the switch that is connected to a Catalyst 5000 switch.

**Figure 5-2** Discovery Through Non-CDP-Capable and Noncluster-Capable Devices

---

Discovery Through Different VLANs

If the cluster command switch is a Catalyst 2970, Catalyst 3550, Catalyst 3560, or Catalyst 3750 switch, the cluster can have cluster member switches in different VLANs. As cluster member switches, they must be connected through at least one VLAN in common with the cluster command switch. The cluster command switch in *Figure 5-3* has ports assigned to VLANs 9, 16, and 62 and therefore discovers the switches in those VLANs. It does not discover the switch in VLAN 50. It also does not discover the switch in VLAN 16 in the first column because the cluster command switch has no VLAN connectivity to it.

Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL cluster member switches must be connected to the cluster command switch through their management VLAN. For information about discovery through management VLANs, see the “Discovery Through Different Management VLANs” section on page 5-8. For more information about VLANs, see Chapter 13, “Configuring VLANs.”
### Discovery Through Different Management VLANs

Catalyst 2970, Catalyst 3550, Catalyst 3560, or Catalyst 3750 cluster command switches can discover and manage cluster member switches in different VLANs and different management VLANs. As cluster member switches, they must be connected through at least one VLAN in common with the cluster command switch. They do not need to be connected to the cluster command switch through their management VLAN. The default management VLAN is VLAN 1.

**Note**

If the switch cluster has a Catalyst 3750 or 2975 switch or has a switch stack, that switch or switch stack must be the cluster command switch.

The cluster command switch and standby command switch in Figure 5-4 (assuming they are Catalyst 2960, Catalyst 2970, Catalyst 2975, Catalyst 3550, Catalyst 3560, or Catalyst 3750 cluster command switches) have ports assigned to VLANs 9, 16, and 62. The management VLAN on the cluster command switch is VLAN 9. Each cluster command switch discovers the switches in the different management VLANs except these:

- Switches 7 and 10 (switches in management VLAN 4) because they are not connected through a common VLAN (meaning VLANs 62 and 9) with the cluster command switch
- Switch 9 because automatic discovery does not extend beyond a noncandidate device, which is switch 7
Discovery Through Routed Ports

If the cluster command switch has a routed port (RP) configured, it discovers only candidate and cluster member switches in the same VLAN as the routed port. For more information about routed ports, see the “Routed Ports” section on page 11-4.

The Layer 3 cluster command switch in Figure 5-5 can discover the switches in VLANs 9 and 62 but not the switch in VLAN 4. If the routed port path between the cluster command switch and cluster member switch 7 is lost, connectivity with cluster member switch 7 is maintained because of the redundant path through VLAN 9.
Discovery of Newly Installed Switches

To join a cluster, the new, out-of-the-box switch must be connected to the cluster through one of its access ports. An access port (AP) carries the traffic of and belongs to only one VLAN. By default, the new switch and its access ports are assigned to VLAN 1.

When the new switch joins a cluster, its default VLAN changes to the VLAN of the immediately upstream neighbor. The new switch also configures its access port to belong to the VLAN of the immediately upstream neighbor.

The cluster command switch in Figure 5-6 belongs to VLANs 9 and 16. When new cluster-capable switches join the cluster:

- One cluster-capable switch and its access port are assigned to VLAN 9.
- The other cluster-capable switch and its access port are assigned to management VLAN 16.
HSRP and Standby Cluster Command Switches

The switch supports Hot Standby Router Protocol (HSRP) so that you can configure a group of standby cluster command switches. Because a cluster command switch manages the forwarding of all communication and configuration information to all the cluster member switches, we strongly recommend the following:

- For a cluster command switch stack, a standby cluster command switch is necessary if the entire switch stack fails. However, if only the stack master in the command switch stack fails, the switch stack elects a new stack master and resumes its role as the cluster command switch stack.
- For a cluster command switch that is a standalone switch, configure a standby cluster command switch to take over if the primary cluster command switch fails.

A cluster standby group is a group of command-capable switches that meet the requirements described in the “Standby Cluster Command Switch Characteristics” section on page 5-3. Only one cluster standby group can be assigned per cluster.

**Note**
The cluster standby group is an HSRP group. Disabling HSRP disables the cluster standby group.

The switches in the cluster standby group are ranked according to HSRP priorities. The switch with the highest priority in the group is the active cluster command switch (AC). The switch with the next highest priority is the standby cluster command switch (SC). The other switches in the cluster standby group are the passive cluster command switches (PC). If the active cluster command switch and the standby cluster command switch become disabled at the same time, the passive cluster command switch with the highest priority becomes the active cluster command switch. For the limitations to automatic discovery, see the “Automatic Recovery of Cluster Configuration” section on page 5-13. For information about changing HSRP priority values, see the “Configuring HSRP Priority” section on page 41-8. The HSRP standby priority interface configuration commands are the same for changing the priority of cluster standby group members and router-redundancy group members.

**Note**
The HSRP standby hold time interval should be greater than or equal to three times the hello time interval. The default HSRP standby hold time interval is 10 seconds. The default HSRP standby hello time interval is 3 seconds. For more information about the standby hold time and standby hello time intervals, see the “Configuring HSRP Authentication and Timers” section on page 41-10.

These connectivity guidelines ensure automatic discovery of the switch cluster, cluster candidates, connected switch clusters, and neighboring edge devices. These topics also provide more detail about standby cluster command switches:

- Virtual IP Addresses, page 5-12
- Other Considerations for Cluster Standby Groups, page 5-12
- Automatic Recovery of Cluster Configuration, page 5-13
Virtual IP Addresses

You need to assign a unique virtual IP address and group number and name to the cluster standby group. This information must be configured on a specific VLAN or routed port on the active cluster command switch. The active cluster command switch receives traffic destined for the virtual IP address. To manage the cluster, you must access the active cluster command switch through the virtual IP address, not through the command-switch IP address. This is in case the IP address of the active cluster command switch is different from the virtual IP address of the cluster standby group.

If the active cluster command switch fails, the standby cluster command switch assumes ownership of the virtual IP address and becomes the active cluster command switch. The passive switches in the cluster standby group compare their assigned priorities to decide the new standby cluster command switch. The passive standby switch with the highest priority then becomes the standby cluster command switch. When the previously active cluster command switch becomes active again, it resumes its role as the active cluster command switch, and the current active cluster command switch becomes the standby cluster command switch again. For more information about IP address in switch clusters, see the “IP Addresses” section on page 5-14.

Other Considerations for Cluster Standby Groups

These requirements also apply:

- Standby cluster command switches must be the same type of switches as the cluster command switch. For example, if the cluster command switch is a Catalyst 3560 switch, the standby cluster command switches must also be Catalyst 3560 switches. Refer to the switch configuration guide of other cluster-capable switches for their requirements on standby cluster command switches.

  If your switch cluster has a Catalyst 3560 switch, it should be the cluster command switch unless the cluster has a Catalyst 3750 switch or switch stack. If the switch cluster has a Catalyst 3750 switch or switch stack, that switch or switch stack must be the cluster command switch.

- Only one cluster standby group can be assigned to a cluster. You can have more than one router-redundancy standby group.

  An HSRP group can be both a cluster standby group and a router-redundancy group. However, if a router-redundancy group becomes a cluster standby group, router redundancy becomes disabled on that group. You can re-enable it by using the CLI. For more information about HSRP and router redundancy, see Chapter 41, “Configuring HSRP.”

- All standby-group members must be members of the cluster.

  There is no limit to the number of switches that you can assign as standby cluster command switches. However, the total number of switches in the cluster—which would include the active cluster command switch, standby-group members, and cluster member switches—cannot be more than 16.

- Each standby-group member (Figure 5-7) must be connected to the cluster command switch through the same VLAN. In this example, the cluster command switch and standby cluster command switches are Catalyst 2970, Catalyst 3550, Catalyst 3560, or Catalyst 3750 cluster command switches. Each standby-group member must also be redundantly connected to each other through at least one VLAN in common with the switch cluster.
Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL cluster member switches must be connected to the cluster standby group through their management VLANs. For more information about VLANs in switch clusters, see these sections:

- “Discovery Through Different VLANs” section on page 5-7
- “Discovery Through Different Management VLANs” section on page 5-8

**Figure 5-7 VLAN Connectivity between Standby-Group Members and Cluster Members**

Automatic Recovery of Cluster Configuration

The active cluster command switch continually forwards cluster-configuration information (but not device-configuration information) to the standby cluster command switch. This ensures that the standby cluster command switch can take over the cluster immediately after the active cluster command switch fails.

Automatic discovery has these limitations:

- This limitation applies only to clusters that have Catalyst 2950, Catalyst 3550, Catalyst 3560, and Catalyst 3750 command and standby cluster command switches: If the active cluster command switch and standby cluster command switch become disabled at the same time, the passive cluster command switch with the highest priority becomes the active cluster command switch. However, because it was a passive standby cluster command switch, the previous cluster command switch did not forward cluster-configuration information to it. The active cluster command switch only forwards cluster-configuration information to the standby cluster command switch. You must therefore rebuild the cluster.

- This limitation applies to all clusters: If the active cluster command switch fails and there are more than two switches in the cluster standby group, the new cluster command switch does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL cluster member switches. You must re-add these cluster member switches to the cluster.

- This limitation applies to all clusters: If the active cluster command switch fails and becomes active again, it does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL cluster member switches. You must again add these cluster member switches to the cluster.
When the previously active cluster command switch resumes its active role, it receives a copy of the latest cluster configuration from the active cluster command switch, including members that were added while it was down. The active cluster command switch sends a copy of the cluster configuration to the cluster standby group.

**IP Addresses**

You must assign IP information to a cluster command switch. You can assign more than one IP address to the cluster command switch, and you can access the cluster through any of the command-switch IP addresses. If you configure a cluster standby group, you must use the standby-group virtual IP address to manage the cluster from the active cluster command switch. Using the virtual IP address ensures that you retain connectivity to the cluster if the active cluster command switch fails and that a standby cluster command switch becomes the active cluster command switch.

If the active cluster command switch fails and the standby cluster command switch takes over, you must either use the standby-group virtual IP address or any of the IP addresses available on the new active cluster command switch to access the cluster.

You can assign an IP address to a cluster-capable switch, but it is not necessary. A cluster member switch is managed and communicates with other cluster member switches through the command-switch IP address. If the cluster member switch leaves the cluster and it does not have its own IP address, you must assign an IP address to manage it as a standalone switch.

For more information about IP addresses, see Chapter 3, “Assigning the Switch IP Address and Default Gateway.”

**Hostnames**

You do not need to assign a host name to either a cluster command switch or an eligible cluster member. However, a hostname assigned to the cluster command switch can help to identify the switch cluster. The default hostname for the switch is *Switch*.

If a switch joins a cluster and it does not have a hostname, the cluster command switch appends a unique member number to its own hostname and assigns it sequentially as each switch joins the cluster. The number means the order in which the switch was added to the cluster. For example, a cluster command switch named *eng-cluster* could name the fifth cluster member *eng-cluster-5*.

If a switch has a hostname, it retains that name when it joins a cluster and when it leaves the cluster.

If a switch received its hostname from the cluster command switch, was removed from a cluster, was then added to a new cluster, and kept the same member number (such as 5), the switch overwrites the old hostname (such as *eng-cluster-5*) with the hostname of the cluster command switch in the new cluster (such as *mkg-cluster-5*). If the switch member number changes in the new cluster (such as 3), the switch retains the previous name (*eng-cluster-5*).

**Passwords**

You do not need to assign passwords to an individual switch if it will be a cluster member. When a switch joins a cluster, it inherits the command-switch password and retains it when it leaves the cluster. If no command-switch password is configured, the cluster member switch inherits a null password. Cluster member switches only inherit the command-switch password.
If you change the member-switch password to be different from the command-switch password and save the change, the switch is not manageable by the cluster command switch until you change the member-switch password to match the command-switch password. Rebooting the member switch does not revert the password back to the command-switch password. We recommend that you do not change the member-switch password after it joins a cluster.

For more information about passwords, see the “Preventing Unauthorized Access to Your Switch” section on page 8-1.

For password considerations specific to the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides for those switches.

**SNMP Community Strings**

A cluster member switch inherits the command-switch first read-only (RO) and read-write (RW) community strings with \(@esN\) appended to the community strings:

- \(command-switch-readonly-community-string@esN\), where \(N\) is the member-switch number.
- \(command-switch-readwrite-community-string@esN\), where \(N\) is the member-switch number.

If the cluster command switch has multiple read-only or read-write community strings, only the first read-only and read-write strings are propagated to the cluster member switch.

The switches support an unlimited number of community strings and string lengths. For more information about SNMP and community strings, see Chapter 31, “Configuring SNMP.”

For SNMP considerations specific to the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides specific to those switches.

**TACACS+ and RADIUS**

If Terminal Access Controller Access Control System Plus (TACACS+) is configured on a cluster member, it must be configured on all cluster members. Similarly, if RADIUS is configured on a cluster member, it must be configured on all cluster members. Further, the same switch cluster cannot have some members configured with TACACS+ and other members configured with RADIUS.

For more information about TACACS+, see the “Controlling Switch Access with TACACS+” section on page 8-10. For more information about RADIUS, see the “Controlling Switch Access with RADIUS” section on page 8-18.

**LRE Profiles**

A configuration conflict occurs if a switch cluster has Long-Reach Ethernet (LRE) switches that use both private and public profiles. If one LRE switch in a cluster is assigned a public profile, all LRE switches in that cluster must have that same public profile. Before you add an LRE switch to a cluster, make sure that you assign it the same public profile used by other LRE switches in the cluster.

A cluster can have a mix of LRE switches that use different private profiles.
Using the CLI to Manage Switch Clusters

You can configure cluster member switches from the CLI by first logging into the cluster command switch. Enter the `rcommand` user EXEC command and the cluster member switch number to start a Telnet session (through a console or Telnet connection) and to access the cluster member switch CLI. The command mode changes, and the Cisco IOS commands operate as usual. Enter the `exit` privileged EXEC command on the cluster member switch to return to the command-switch CLI.

This example shows how to log into member-switch 3 from the command-switch CLI:

```
switch# rcommand 3
```

If you do not know the member-switch number, enter the `show cluster members` privileged EXEC command on the cluster command switch. For more information about the `rcommand` command and all other cluster commands, refer to the switch command reference.

The Telnet session accesses the member-switch CLI at the same privilege level as on the cluster command switch. The Cisco IOS commands then operate as usual. For instructions on configuring the switch for a Telnet session, see the “Disabling Password Recovery” section on page 8-5.

Catalyst 1900 and Catalyst 2820 CLI Considerations

If your switch cluster has Catalyst 1900 and Catalyst 2820 switches running standard edition software, the Telnet session accesses the management console (a menu-driven interface) if the cluster command switch is at privilege level 15. If the cluster command switch is at privilege level 1 to 14, you are prompted for the password to access the menu console.

Command-switch privilege levels map to the Catalyst 1900 and Catalyst 2820 cluster member switches running standard and Enterprise Edition Software as follows:

- If the command-switch privilege level is 1 to 14, the cluster member switch is accessed at privilege level 1.
- If the command-switch privilege level is 15, the cluster member switch is accessed at privilege level 15.

**Note**

The Catalyst 1900 and Catalyst 2820 CLI is available only on switches running Enterprise Edition Software.

For more information about the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides for those switches.

Using SNMP to Manage Switch Clusters

When you first power on the switch, SNMP is enabled if you enter the IP information by using the setup program and accept its proposed configuration. If you did not use the setup program to enter the IP information and SNMP was not enabled, you can enable it as described in the “Configuring SNMP” section on page 31-6. On Catalyst 1900 and Catalyst 2820 switches, SNMP is enabled by default.

When you create a cluster, the cluster command switch manages the exchange of messages between cluster member switches and an SNMP application. The cluster software on the cluster command switch appends the cluster member switch number (`@esN`, where `N` is the switch number) to the first configured read-write and read-only community strings on the cluster command switch and propagates them to the
cluster member switch. The cluster command switch uses this community string to control the forwarding of gets, sets, and get-next messages between the SNMP management station and the cluster member switches.

**Note**

When a cluster standby group is configured, the cluster command switch can change without your knowledge. Use the first read-write and read-only community strings to communicate with the cluster command switch if there is a cluster standby group configured for the cluster.

If the cluster member switch does not have an IP address, the cluster command switch redirects traps from the cluster member switch to the management station, as shown in Figure 5-8. If a cluster member switch has its own IP address and community strings, the cluster member switch can send traps directly to the management station, without going through the cluster command switch.

If a cluster member switch has its own IP address and community strings, they can be used in addition to the access provided by the cluster command switch. For more information about SNMP and community strings, see Chapter 31, “Configuring SNMP.”

**Figure 5-8  SNMP Management for a Cluster**
Administering the Switch

This chapter describes how to perform one-time operations to administer the Catalyst 3560 switch. This chapter consists of these sections:

- Managing the System Time and Date, page 6-1
- Configuring a System Name and Prompt, page 6-14
- Creating a Banner, page 6-17
- Managing the MAC Address Table, page 6-19
- Managing the ARP Table, page 6-30

Managing the System Time and Date

You can manage the system time and date on your switch using automatic configuration, such as the Network Time Protocol (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 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

These sections contain this configuration information:

- Understanding the System Clock, page 6-1
- Understanding Network Time Protocol, page 6-2
- Configuring NTP, page 6-4
- Configuring Time and Date Manually, page 6-11

Understanding the System Clock

The heart 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:

- 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 Universal Time Coordinated (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. For configuration information, see the “Configuring Time and Date Manually” section on page 6-11.

### Understanding 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.
Figure 6-1 shows a typical network example using NTP. Switch A is the NTP master, with Switches 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, 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.
Configuring NTP

The switch does not have a hardware-supported clock and cannot function as an NTP master clock to which peers synchronize themselves when an external NTP source is not available. The switch also has no hardware support for a calendar. As a result, the ntp update-calendar and the ntp master global configuration commands are not available.

These sections contain this configuration information:
- Default NTP Configuration, page 6-4
- Configuring NTP Authentication, page 6-5
- Configuring NTP Associations, page 6-6
- Configuring NTP Broadcast Service, page 6-7
- Configuring NTP Access Restrictions, page 6-8
- Configuring the Source IP Address for NTP Packets, page 6-10
- Displaying the NTP Configuration, page 6-11

Default NTP Configuration

Table 6-1 shows the default NTP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP authentication</td>
<td>Disabled. No authentication key is specified.</td>
</tr>
<tr>
<td>NTP peer or server associations</td>
<td>None configured.</td>
</tr>
<tr>
<td>NTP broadcast service</td>
<td>Disabled; no interface sends or receives NTP broadcast packets.</td>
</tr>
<tr>
<td>NTP access restrictions</td>
<td>No access control is specified.</td>
</tr>
<tr>
<td>NTP packet source IP address</td>
<td>The source address is set by the outgoing interface.</td>
</tr>
</tbody>
</table>

NTP is enabled on all interfaces by default. All interfaces receive NTP packets.
Configuring NTP Authentication

This procedure must be coordinated with the administrator of the NTP server; the information you configure in this procedure must be matched by the servers used by the switch to synchronize its time to the NTP server.

Beginning in privileged EXEC mode, follow these steps to authenticate the associations (communications between devices running NTP that provide for accurate timekeeping) with other devices for security purposes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ntp authenticate</td>
<td>Enable the NTP authentication feature, which is disabled by default.</td>
</tr>
<tr>
<td>3</td>
<td>ntp authentication-key number md5 value</td>
<td>Define the authentication keys. By default, none are defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For number, specify a key number. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• md5 specifies that message authentication support is provided by using the message digest algorithm 5 (MD5).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For value, enter an arbitrary string of up to eight characters for the key.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The switch does not synchronize to a device unless both have one of these authentication keys, and the key number is specified by the ntp trusted-key key-number command.</td>
</tr>
<tr>
<td>4</td>
<td>ntp trusted-key key-number</td>
<td>Specify one or more key numbers (defined in Step 3) that a peer NTP device must provide in its NTP packets for this switch to synchronize to it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no trusted keys are defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For key-number, specify the key defined in Step 3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This command provides protection against accidentally synchronizing the switch to a device that is not trusted.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable NTP authentication, use the no ntp authenticate global configuration command. To remove an authentication key, use the no ntp authentication-key number global configuration command. To disable authentication of the identity of a device, use the no ntp trusted-key key-number global configuration command.

This example shows how to configure the switch to synchronize only to devices providing authentication key 42 in the device’s NTP packets:

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
```
Configuring NTP Associations

An NTP association can be a peer association (this switch can either synchronize to the other device or allow the other device to synchronize to it), or it can be a server association (meaning that only this switch synchronizes to the other device, and not the other way around).

Beginning in privileged EXEC mode, follow these steps to form an NTP association with another device:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: ntp peer ip-address [version number] [key keyid] [source interface] [prefer] or ntp server ip-address [version number] [key keyid] [source interface] [prefer]</td>
<td>Configure the switch system clock to synchronize a peer or to be synchronized by a peer (peer association). or Configure the switch system clock to be synchronized by a time server (server association).</td>
</tr>
<tr>
<td>Step 3: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4: show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

You need to configure only one end of an association; the other device can automatically establish the association. If you are using the default NTP version (Version 3) and NTP synchronization does not occur, try using NTP Version 2. Many NTP servers on the Internet run Version 2.

To remove a peer or server association, use the `no ntp peer ip-address` or the `no ntp server ip-address` global configuration command.

This example shows how to configure the switch to synchronize its system clock with the clock of the peer at IP address 172.16.22.44 using NTP Version 2:

```
Switch(config)# ntp server 172.16.22.44 version 2
```
Configuring NTP Broadcast Service

The communications between devices running NTP (known as associations) are usually statically configured; each device is given the IP addresses 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, the information flow is one-way only.

The switch can send or receive NTP broadcast packets on an interface-by-interface basis if there is an NTP broadcast server, such as a router, broadcasting time information on the network. The switch can send NTP broadcast packets to a peer so that the peer can synchronize to it. The switch can also receive NTP broadcast packets to synchronize its own clock. This section provides procedures for both sending and receiving NTP broadcast packets.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send NTP broadcast packets to peers so that they can synchronize their clock to the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the interface to send NTP broadcast packets, and enter interface configuration mode.</td>
</tr>
<tr>
<td>ntp broadcast [version number] [key keyid] [destination-address]</td>
<td>Enable the interface to send NTP broadcast packets to a peer. By default, this feature is disabled on all interfaces.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For number, specify the NTP version number. The range is 1 to 3. If you do not specify a version, Version 3 is used.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For keyid, specify the authentication key to use when sending packets to the peer.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For destination-address, specify the IP address of the peer that is synchronizing its clock to this switch.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>Configure the connected peers to receive NTP broadcast packets as described in the next procedure.</td>
<td></td>
</tr>
</tbody>
</table>

To disable the interface from sending NTP broadcast packets, use the `no ntp broadcast` interface configuration command.

This example shows how to configure a port to send NTP Version 2 packets:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast version 2
```
Beginning in privileged EXEC mode, follow these steps to configure the switch to receive NTP broadcast packets from connected peers:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ntp broadcast client</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ntp broadcastdelay microseconds</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable an interface from receiving NTP broadcast packets, use the `no ntp broadcast client` interface configuration command. To change the estimated round-trip delay to the default, use the `no ntp broadcastdelay` global configuration command.

This example shows how to configure a port to receive NTP broadcast packets:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ntp broadcast client
```

### Configuring NTP Access Restrictions

You can control NTP access on two levels as described in these sections:

- Creating an Access Group and Assigning a Basic IP Access List, page 6-9
- Disabling NTP Services on a Specific Interface, page 6-10
Creating an Access Group and Assigning a Basic IP Access List

Beginning in privileged EXEC mode, follow these steps to control access to NTP services by using access lists:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ntp access-group { query-only</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></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>access-list access-list-number permit source [source-wildcard]</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>Note</td>
<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>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

The access group keywords are scanned in this order, from least restrictive to most restrictive:

1. peer—Allows time requests and NTP control queries and allows the switch to synchronize itself to a device whose address passes the access list criteria.
2. serve—Allows time requests and NTP control queries, but does not allow the switch to synchronize itself to a device whose address passes the access list criteria.
3. serve-only—Allows only time requests from a device whose address passes the access list criteria.
4. query-only—Allows only NTP control queries from a device whose address passes the access list criteria.

If the source IP address matches the access lists for more than one access type, the first type is granted. If no access groups are specified, all access types are granted to all devices. If any access groups are specified, only the specified access types are granted.
To remove access control to the switch NTP services, use the `no ntp access-group {query-only | serve-only | serve | peer} global configuration command.

This example shows how to configure the switch to allow itself to synchronize to a peer from access list 99. However, the switch restricts access to allow only time requests from access list 42:

```
Switch# configure terminal
Switch(config)# ntp access-group peer 99
Switch(config)# ntp access-group serve-only 42
Switch(config)# access-list 99 permit 172.20.130.5
Switch(config)# access-list 42 permit 172.20.130.6
```

### Disabling NTP Services on a Specific Interface

NTP services are enabled on all interfaces by default.

Beginning in privileged EXEC mode, follow these steps to disable NTP packets from being received on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 <code>interface interface-id</code></td>
<td>Enter interface configuration mode, and specify the interface to disable.</td>
</tr>
<tr>
<td>Step 3 <code>ntp disable</code></td>
<td>Disable NTP packets from being received on the interface. By default, all interfaces receive NTP packets.</td>
</tr>
<tr>
<td>Step 4 <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 <code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To re-enable receipt of NTP packets on an interface, use the `no ntp disable` interface configuration command.

### Configuring the Source IP Address for NTP Packets

When the switch sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use the `ntp source` global configuration command when you want to use a particular source IP address for all NTP packets. The address is taken from the specified interface. This command is useful if the address on an interface cannot be used as the destination for reply packets.

Beginning in privileged EXEC mode, follow these steps to configure a specific interface from which the IP source address is to be taken:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 <code>ntp source type number</code></td>
<td>Specify the interface type and number from which the IP source address is taken. By default, the source address is set by the outgoing interface.</td>
</tr>
<tr>
<td>Step 3 <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
The specified interface is used for the source address for all packets sent to all destinations. If a source address is to be used for a specific association, use the `source` keyword in the `ntp peer` or `ntp server` global configuration command as described in the “Configuring NTP Associations” section on page 6-6.

### Displaying the NTP Configuration

You can use two privileged EXEC commands to display NTP information:

- `show ntp associations [detail]`
- `show ntp status`

**Note**
For detailed information about the fields in these displays, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

### Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the switch can synchronize, you do not need to manually set the system clock.

These sections contain this configuration information:

- Setting the System Clock, page 6-11
- Displaying the Time and Date Configuration, page 6-12
- Configuring the Time Zone, page 6-12
- Configuring Summer Time (Daylight Saving Time), page 6-13

### 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.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to set the system clock:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>clock set ( hh:mm:ss ) day month year</td>
</tr>
<tr>
<td>or</td>
<td>clock set ( hh:mm:ss ) month day year</td>
</tr>
<tr>
<td>Step 1</td>
<td>Manually set the system clock using one of these formats.</td>
</tr>
<tr>
<td></td>
<td>• For ( hh:mm:ss ), specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone.</td>
</tr>
<tr>
<td></td>
<td>• For day, specify the day by date in the month.</td>
</tr>
<tr>
<td></td>
<td>• For month, specify the month by name.</td>
</tr>
<tr>
<td></td>
<td>• For year, specify the year (no abbreviation).</td>
</tr>
</tbody>
</table>

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001:

Switch# clock set 13:32:00 23 July 2001

### Displaying the Time and Date Configuration

To display the time and date configuration, use the `show clock` [detail] privileged EXEC command. The system clock keeps an authoritative flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the authoritative flag is set, the flag prevents peers from synchronizing to the clock when the peers’ time is invalid.

The symbol that precedes the `show clock` display has this meaning:

- *—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

### Configuring the Time Zone

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>clock timezone zone hours-offset [minutes-offset]</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 1</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set the time zone.</td>
</tr>
<tr>
<td></td>
<td>The switch keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set.</td>
</tr>
<tr>
<td></td>
<td>• For zone, enter 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>• For hours-offset, enter the hours offset from UTC.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For minutes-offset, enter the minutes offset from UTC.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
The minutes-offset variable in the clock timezone global configuration command is available for those cases where a local time zone is a percentage of an hour different from UTC. For example, the time zone for some sections of Atlantic Canada (AST) is UTC-3.5, where the 3 means 3 hours and .5 means 50 percent. In this case, the necessary command is `clock timezone AST -3 30`.

To set the time to UTC, use the `no clock timezone` global configuration command.

### Configuring Summer Time (Daylight Saving Time)

Beginning in privileged EXEC mode, follow these steps to configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 clock summer-time zone recurring</td>
<td>Configure summer time to start and end on the specified days every year.</td>
</tr>
<tr>
<td></td>
<td>Summer time is disabled by default. If you specify clock summer-time</td>
</tr>
<tr>
<td></td>
<td>zone recurring without parameters, the summer time rules default to the</td>
</tr>
<tr>
<td></td>
<td>United States rules.</td>
</tr>
<tr>
<td></td>
<td>• For zone, specify the name of the time zone (for example, PDT) to be</td>
</tr>
<tr>
<td></td>
<td>displayed when summer time is in effect.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For week, specify the week of the month (1 to 5 or last).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For day, specify the day of the week (Sunday, Monday...).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For month, specify the month (January, February...).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For hh:mm, specify the time (24-hour format) in hours and</td>
</tr>
<tr>
<td></td>
<td>minutes.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For offset, specify the number of minutes to add during</td>
</tr>
<tr>
<td></td>
<td>summer time. The default is 60.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

The first part of the clock summer-time global configuration command specifies when summer time begins, and the second part specifies when it ends. 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. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

This example shows how to specify that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00:

```
Switch(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```
Beginning in privileged EXEC mode, 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):

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td><code>clock summer-time zone date [month date year hh:mm month date year hh:mm [offset]]</code></td>
<td>Configure summer time to start on the first date and end on the second date.</td>
</tr>
<tr>
<td>or <code>clock summer-time zone date [date month year hh:mm date month year hh:mm [offset]]</code></td>
<td>Summer time is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>• For <code>zone</code>, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>week</code>, specify the week of the month (1 to 5 or <code>last</code>).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>day</code>, specify the day of the week (Sunday, Monday...).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>month</code>, specify the month (January, February...).</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>hh:mm</code>, specify the time (24-hour format) in hours and minutes.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>offset</code>, specify the number of minutes to add during summer time. The default is 60.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

The first part of the `clock summer-time` global configuration command specifies when summer time begins, and the second part specifies when it ends. 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. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

To disable summer time, use the `no clock summer-time` global configuration command.

This example shows how to set summer time to start on October 12, 2000, at 02:00, and end on April 26, 2001, at 02:00:

```
Switch(config)# clock summer-time pdt date 12 October 2000 02:00 26 April 2001 02:00
```

### Configuring a 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, from the Cisco.com page, select **Documentation > Cisco IOS Software > 12.2 Mainline > Command References** and see the **Cisco IOS Configuration Fundamentals Command Reference** and the **Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols**.
These sections contain this configuration information:

- Default System Name and Prompt Configuration, page 6-15
- Configuring a System Name, page 6-15
- Understanding DNS, page 6-15

Default System Name and Prompt Configuration

The default switch system name and prompt is *Switch*.

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

<table>
<thead>
<tr>
<th>Command</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> hostname name</td>
<td>Manually configure a system name.</td>
</tr>
<tr>
<td></td>
<td>The default setting is <em>switch</em>.</td>
</tr>
<tr>
<td></td>
<td>The name must follow the rules for ARPANET hostnames. They must start</td>
</tr>
<tr>
<td></td>
<td>with a letter, end with a letter or digit, and have as interior</td>
</tr>
<tr>
<td></td>
<td>characters only letters, digits, and hyphens. Names can be up to 63</td>
</tr>
<tr>
<td></td>
<td>characters.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show running-config</td>
<td>Verify your entries.</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>
</tbody>
</table>

When you set the system name, it is also used as the system prompt.

To return to the default hostname, use the **no hostname** global configuration command.

Understanding 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.
These sections contain this configuration information:

- Default DNS Configuration, page 6-16
- Setting Up DNS, page 6-16
- Displaying the DNS Configuration, page 6-17

Default DNS Configuration

Table 6-2 shows the default DNS configuration.

<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>

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up your switch to use the DNS:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip domain-name name</td>
<td>Define a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot-up time, no domain name is configured; however, if the switch configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).</td>
</tr>
<tr>
<td>Step 3 ip name-server server-address1 [server-address2 ... server-address6]</td>
<td>Specify the address of one or more name servers to use for name and address resolution. 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.</td>
</tr>
<tr>
<td>Step 4 ip domain-lookup</td>
<td>(Optional) Enable DNS-based hostname-to-address translation on your switch. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner displays 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 also displays on all connected terminals. It appears after the MOTD banner and before the login prompts.

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

These sections contain this configuration information:
- Default Banner Configuration, page 6-17
- Configuring a Message-of-the-Day Login Banner, page 6-18
- Configuring a Login Banner, page 6-19

Default Banner Configuration

The MOTD and login banners are not configured.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

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.

To remove a domain name, use the `no ip domain-name name` global configuration command. To remove a name server address, use the `no ip name-server server-address` global configuration command. To disable DNS on the switch, use the `no ip domain-lookup` global configuration command.

Displaying the DNS Configuration

To display the DNS configuration information, use the `show running-config` privileged EXEC command.
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.

Beginning in privileged EXEC mode, follow these steps to configure a MOTD login banner:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 banner motd c message c</td>
<td>Specify the message of the day.</td>
</tr>
<tr>
<td></td>
<td>For c, enter the delimiting character of your choice, for example, a</td>
</tr>
<tr>
<td></td>
<td>pound sign (#), and press the Return key. The delimiting character</td>
</tr>
<tr>
<td></td>
<td>signifies the beginning and end of the banner text. Characters after the</td>
</tr>
<tr>
<td></td>
<td>ending delimiter are discarded.</td>
</tr>
<tr>
<td></td>
<td>For message, enter a banner message up to 255 characters. You cannot</td>
</tr>
<tr>
<td></td>
<td>use the delimiting character in the message.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete the MOTD banner, use the no banner motd global configuration command.

This example shows how to configure a MOTD banner for the switch 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 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```
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.

Beginning in privileged EXEC mode, follow these steps to configure a login banner:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>banner login $ message $</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To delete the login banner, use the no banner login global configuration command.

This example shows how to configure a login banner for the switch 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)#
```

Managing the MAC Address Table

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address: a source MAC address that the switch learns and then ages when it is not in use.
- Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address and the type (static or dynamic).

Note

For complete syntax and usage information for the commands used in this section, see the command reference for this release.
These sections contain this configuration information:

- Building the Address Table, page 6-20
- MAC Addresses and VLANs, page 6-20
- Default MAC Address Table Configuration, page 6-21
- Changing the Address Aging Time, page 6-21
- Removing Dynamic Address Entries, page 6-22
- Configuring MAC Address Change Notification Traps, page 6-22
- Configuring MAC Address Move Notification Traps, page 6-24
- Configuring MAC Threshold Notification Traps, page 6-25
- Adding and Removing Static Address Entries, page 6-26
- Configuring Unicast MAC Address Filtering, page 6-27
- Disabling MAC Address Learning on a VLAN, page 6-28
- Displaying Address Table Entries, page 6-30

**Building the Address Table**

With multiple MAC addresses supported on all ports, you can connect any port on the switch to individual workstations, repeaters, switches, routers, or 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 stations 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.
When private VLANs are configured, address learning depends on the type of MAC address:

- Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a private-VLAN secondary VLAN is replicated in the primary VLAN.

- Static MAC addresses configured in a primary or secondary VLAN are not replicated in the associated VLANs. When you configure a static MAC address in a private VLAN primary or secondary VLAN, you should also configure the same static MAC address in all associated VLANs.

For more information about private VLANs, see Chapter 15, “Configuring Private VLANs.”

## Default MAC Address Table Configuration

Table 6-3 shows the default MAC address table configuration.

<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>

### Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned. Flooding results, which can impact switch performance.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mac address-table aging-time [0</td>
<td>Set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. 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. For vlan-id, valid IDs are 1 to 4094.</td>
</tr>
<tr>
<td>10-1000000] [vlan vlan-id]</td>
<td></td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show mac address-table aging-time</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To return to the default value, use the `no mac address-table aging-time` global configuration command.

### Removing Dynamic Address Entries

To remove all dynamic entries, use the `clear mac address-table dynamic` command in privileged EXEC mode. You can also remove a specific MAC address (clear mac address-table dynamic address mac-address), remove all addresses on the specified physical port or port channel (clear mac address-table dynamic interface interface-id), or remove all addresses on a specified VLAN (clear mac address-table dynamic vlan vlan-id).

To verify that dynamic entries have been removed, use the `show mac address-table dynamic` privileged EXEC command.

### Configuring MAC Address Change Notification Traps

MAC address change notification tracks users on a network by storing the MAC address change activity. When the switch learns or removes a MAC address, an SNMP notification trap can be sent to the NMS. If you have many users coming and going from the network, you can set a trap-interval time to bundle the notification traps to reduce network traffic. The MAC notification history table stores MAC address activity for each port for which the trap is set. MAC address change notifications are generated for dynamic and secure MAC addresses. Notifications are not generated for self addresses, multicast addresses, or other static addresses.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send MAC address change notification traps to an NMS host:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| 2    | snmp-server host host-addr {traps | informs} {version {1 | 2c | 3}} community-string notification-type | Specify the recipient of the trap message.  
|     |         | • For `host-addr`, specify the name or address of the NMS.  
|     |         | • Specify `traps` (the default) to send SNMP traps to the host. Specify `informs` to send SNMP informs to the host.  
|     |         | • Specify the SNMP version to support. Version 1, the default, is not available with informs.  
|     |         | • For `community-string`, specify 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.  
|     |         | • For `notification-type`, use the `mac-notification` keyword. |
| 3    | snmp-server enable traps mac-notification change | Enable the switch to send MAC address change notification traps to the NMS. |
To disable MAC address-change notification traps, use the `no snmp-server enable traps mac-notification change` global configuration command. To disable the MAC address-change notification traps on a specific interface, use the `no snmp trap mac-notification change {added | removed}` interface configuration command. To disable the MAC address-change notification feature, use the `no mac address-table notification change` global configuration command.

This example shows how to specify 172.20.10.10 as the NMS, enable the switch to send 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 gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification change added
```

You can verify your settings by entering the `show mac address-table notification change interface` and the `show mac address-table notification change` privileged EXEC commands.
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.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send MAC address-move notification traps to an NMS host:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>snmp-server host host-addr {traps</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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>snmp-server enable traps mac-notification move</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>mac address-table notification mac-move</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show mac address-table notification mac-move</td>
</tr>
<tr>
<td>show running-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.

This example shows how to specify 172.20.10.10 as the NMS, enable the switch to send MAC address move notification traps to the NMS, enable the MAC address move notification feature, and enable traps when a MAC address moves from one port to another.

```
Switch(config)# snmp-server host 172.20.10.10 traps private mac-notification
Switch(config)# snmp-server enable traps mac-notification move
Switch(config)# mac address-table notification mac-move
```

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.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send MAC address table threshold notification traps to an NMS host:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server host host-addr {traps</td>
<td>informs} {version {1</td>
<td>2c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For host-addr, specify the name or address of the NMS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specify traps (the default) to send SNMP traps to the host. Specify informs to send SNMP informs to the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Specify the SNMP version to support. Version 1, the default, is not available with informs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For community-string, specify 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For notification-type, use the mac-notification keyword.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server enable traps mac-notification threshold</td>
<td>Enable the switch to send MAC threshold notification traps to the NMS.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac address-table notification threshold</td>
<td>Enable the MAC address threshold notification feature.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac address-table notification threshold [limit percentage]</td>
<td>Enter the threshold value for the MAC address threshold usage monitoring.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For limit percentage, specify the percentage of the MAC address table use; valid values are from 1 to 100 percent. The default is 50 percent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For interval time, specify the time between notifications; valid values are greater than or equal to 120 seconds. The default is 120 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mac address-table notification threshold</td>
<td>Verify your entries.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>
To disable MAC address-threshold notification traps, use the `no snmp-server enable traps mac-notification threshold` global configuration command. To disable the MAC address-threshold notification feature, use the `no mac address-table notification threshold` global configuration command.

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
```

You can verify your settings by entering the `show mac address-table notification threshold` privileged EXEC commands.

### Adding and Removing Static Address Entries

A static address has these characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

You can add and remove static addresses and define the forwarding behavior for them. The forwarding behavior defines how a port that receives a packet forwards it to another port for transmission. Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you specify. You can specify a different list of destination ports for each source port.

A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

You add a static address to the address table by specifying the destination MAC unicast address and the VLAN from which it is received. Packets received with this destination address are forwarded to the interface specified with the `interface-id` option.

When you configure a static MAC address in a private-VLAN primary or secondary VLAN, you should also configure the same static MAC address in all associated VLANs. Static MAC addresses configured in a private-VLAN primary or secondary VLAN are not replicated in the associated VLAN. For more information about private VLANs, see Chapter 15, “Configuring Private VLANs.”
Beginning in privileged EXEC mode, follow these steps to add a static address:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 mac address-table static mac-addr vlan vlan-id interface interface-id | Add a static address to the MAC address table.  
- For mac-addr, specify 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.  
- For vlan-id, specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.  
- For interface-id, specify the interface to which the received packet is forwarded. Valid interfaces include physical ports or port channels. For static multicast addresses, you can enter multiple interface IDs. For static unicast addresses, you can enter only one interface at a time, but you can enter the command multiple times with the same MAC address and VLAN ID. |
| Step 3 end | Return to privileged EXEC mode. |
| Step 4 show mac address-table static | Verify your entries. |
| Step 5 copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To remove static entries from the address table, use the no mac address-table static mac-addr vlan vlan-id [interface interface-id] global configuration command.

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 gigabitethernet0/1
```

**Configuring Unicast MAC Address Filtering**

When unicast MAC address filtering is enabled, the switch drops packets with specific source or destination MAC addresses. This feature is disabled by default and only supports unicast static addresses.

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. If you specify one of these addresses when entering the mac address-table static mac-addr vlan vlan-id drop global configuration command, one of these messages appears:
  
  % Only unicast addresses can be configured to be dropped

  % CPU destined address cannot be configured as drop address

- Packets that are forwarded to the CPU are also not supported.
Managing the MAC Address Table

If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

For example, if you enter the `mac address-table static mac-addr vlan vlan-id interface interface-id` global configuration command followed by the `mac address-table static mac-addr vlan vlan-id drop` command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the `mac address-table static mac-addr vlan vlan-id drop` global configuration command followed by the `mac address-table static mac-addr vlan vlan-id interface interface-id` command, the switch adds the MAC address as a static address.

You enable unicast MAC address filtering and configure the switch to drop packets with a specific address by specifying the source or destination unicast MAC address and the VLAN from which it is received.

Beginning in privileged EXEC mode, follow these steps to configure the switch to drop a source or destination unicast static address:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 mac address-table static mac-addr vlan vlan-id drop | Enable unicast MAC address filtering and configure the switch to drop a packet with the specified source or destination unicast static address.  
  • For `mac-addr`, specify a source or destination unicast MAC address.  
  • For `vlan-id`, specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. |
| Step 3 end                               | Return to privileged EXEC mode.                                          |
| Step 4 show mac address-table static    | Verify your entries.                                                    |
| Step 5 copy running-config startup-config | (Optional) Save your entries in the configuration file.                 |

To disable unicast MAC address filtering, use the `no mac address-table static mac-addr vlan vlan-id` global configuration command.

This example shows how to enable unicast MAC address filtering and to configure the switch to 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
```

Disabling MAC Address Learning on a VLAN

By default, MAC address learning is enabled on all VLANs on the switch. You can control MAC address learning on a VLAN to manage the available MAC address table space by controlling which VLANs, and therefore which ports, can learn MAC addresses. Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network.
Follow these guidelines when disabling MAC address learning on a VLAN:

- Use caution before disabling MAC address learning on a VLAN with a configured switch virtual interface (SVI). The switch then floods all IP packets in the Layer 2 domain.

- You can disable MAC address learning on a single VLAN ID (for example, `no mac address-table learning vlan 223`) or on a range of VLAN IDs (for example, `no mac address-table learning vlan 1-20, 15`).

- We recommend that you disable MAC address learning only in VLANs with two ports. If you disable MAC address learning on a VLAN with more than two ports, every packet entering the switch is flooded in that VLAN domain.

- You cannot disable MAC address learning on a VLAN that is used internally by the switch. If the VLAN ID that you enter is an internal VLAN, the switch generates an error message and rejects the command. To view internal VLANs in use, enter the `show vlan internal usage` privileged EXEC command.

- If you disable MAC address learning on a VLAN configured as a private-VLAN primary VLAN, MAC addresses are still learned on the secondary VLAN that belongs to the private VLAN and are then replicated on the primary VLAN. If you disable MAC address learning on the secondary VLAN, but not the primary VLAN of a private VLAN, MAC address learning occurs on the primary VLAN and is replicated on the secondary VLAN.

- You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

- If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on that port. If you disable port security, the configured MAC address learning state is enabled.

Beginning in privileged EXEC mode, follow these steps to disable MAC address learning on a VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no mac address-table learning vlan vlan-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mac address-table learning [vlan vlan-id]</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To reenable MAC address learning on a VLAN, use the `default mac address-table learning vlan vlan-id` global configuration command. You can also reenable MAC address learning on a VLAN by entering the `mac address-table learning vlan vlan-id` global configuration command. The first `(default)` command returns to a default condition and therefore does not appear in the output from the `show running-config` command. The second command causes the configuration to appear in the `show running-config` privileged EXEC command display.

This example shows how to disable MAC address learning on VLAN 200:

```
Switch(config)# no mac address-table learning vlan 200
```

You can display the MAC address learning status of all VLANs or a specified VLAN by entering the `show mac-address-table learning [vlan vlan-id]` privileged EXEC command.
Displaying Address Table Entries

You can display the MAC address table by using one or more of the privileged EXEC commands described in Table 6-4:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp snooping groups</td>
<td>Displays the Layer 2 multicast entries for all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table address</td>
<td>Displays MAC address table information for the specified MAC address.</td>
</tr>
<tr>
<td>show mac address-table aging-time</td>
<td>Displays the aging time in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table count</td>
<td>Displays the number of addresses present in all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table dynamic</td>
<td>Displays only dynamic MAC address table entries.</td>
</tr>
<tr>
<td>show mac address-table interface</td>
<td>Displays the MAC address table information for the specified interface.</td>
</tr>
<tr>
<td>show mac address-table learning</td>
<td>Displays MAC address learning status of all VLANs or the specified VLAN.</td>
</tr>
<tr>
<td>show mac address-table notification</td>
<td>Displays the MAC notification parameters and history table.</td>
</tr>
<tr>
<td>show mac address-table static</td>
<td>Displays only static MAC address table entries.</td>
</tr>
<tr>
<td>show mac address-table vlan</td>
<td>Displays the MAC address table information for the specified VLAN.</td>
</tr>
</tbody>
</table>

Managing the ARP Table

To communicate with a device (over Ethernet, for example), the software first must learn the 48-bit MAC address or the local data link address of that device. The process of learning the local data link address from an IP address is called address resolution.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Using an IP address, ARP finds the associated MAC address. When a MAC address is found, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the arpa keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

Note: For CLI procedures, see the Cisco IOS Release 12.2 documentation from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline.
Configuring SDM Templates

You can use SDM templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can select a template to provide maximum system usage for some functions or use the default template to balance resources.

To allocate ternary content addressable memory (TCAM) resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features. You can select SDM templates to optimize these features:

- **Access**—The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- **Default**—The default template gives balance to all functions.
- **Routing**—The routing template maximizes system resources for IPv4 unicast routing, typically required for a router or aggregator in the center of a network.
- **VLANs**—The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.

In addition, the dual IPv4 and IPv6 templates enable a dual stack environment. See the “Dual IPv4 and IPv6 SDM Templates” section on page 7-2.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Access</th>
<th>Default</th>
<th>Routing</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast MAC addresses</td>
<td>4 K</td>
<td>6 K</td>
<td>3 K</td>
<td>12 K</td>
</tr>
<tr>
<td>IGMP groups and multicast routes</td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Unicast routes</td>
<td>6 K</td>
<td>8 K</td>
<td>11 K</td>
<td>0</td>
</tr>
<tr>
<td>• Directly connected hosts</td>
<td>4 K</td>
<td>6 K</td>
<td>3 K</td>
<td>0</td>
</tr>
<tr>
<td>• Indirect routes</td>
<td>2 K</td>
<td>2 K</td>
<td>8 K</td>
<td>0</td>
</tr>
</tbody>
</table>
Chapter 7  Configuring SDM Templates

Understanding the SDM Templates

The first eight rows in the tables (unicast MAC addresses through security ACEs) represent approximate hardware boundaries set when a template is selected. If a section of a hardware resource is full, all processing overflow is sent to the CPU, seriously impacting switch performance. The last row is a guideline used to calculate hardware resource consumption related to the number of Layer 2 VLANs on the switch.

Dual IPv4 and IPv6 SDM Templates

You can select SDM templates to support IP Version 6 (IPv6). For more information about IPv6 and how to configure IPv6 routing, see Chapter 37, “Configuring IP Unicast Routing.”

This software release does not support Policy-Based Routing (PBR) when forwarding IPv6 traffic. The software supports IPv4 PBR only when the dual-ipv4-and-ipv6 routing template is configured.

The dual IPv4 and IPv6 templates allow the switch to be used in dual stack environments (supporting both IPv4 and IPv6). Using the dual stack templates results in less TCAM capacity allowed for each resource. Do not use them if you plan to forward only IPv4 traffic.

These SDM templates support IPv4 and IPv6 environments:

- Dual IPv4 and IPv6 default template—supports Layer 2, multicast, routing, QoS, and ACLs for IPv4; and Layer 2, routing, and ACLs for IPv6.
- Dual IPv4 and IPv6 routing template—supports Layer 2, multicast, routing (including policy-based routing), QoS, and ACLs for IPv4; and Layer 2, routing, and ACLs for IPv6.
- Dual IPv4 and IPv6 VLAN template—supports basic Layer 2, multicast, QoS, and ACLs for IPv4, and basic Layer 2 and ACLs for IPv6.

An IPv4 route requires only one TCAM entry. Because of the hardware compression scheme used for IPv6, an IPv6 route can take more than one TCAM entry, reducing the number of entries forwarded in hardware. For example, for IPv6 directly connected IP addresses, the desktop template might allow less than two thousand entries.

### Table 7-1  Approximate Number of Feature Resources Allowed by Each Template (continued)

<table>
<thead>
<tr>
<th>Resource</th>
<th>Access</th>
<th>Default</th>
<th>Routing</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy-based routing ACEs</td>
<td>512</td>
<td>0</td>
<td>512</td>
<td>0</td>
</tr>
<tr>
<td>QoS classification ACEs</td>
<td>512</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Security ACEs</td>
<td>2 K</td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Layer 2 VLANs</td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
</tbody>
</table>

### Table 7-2  Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast MAC addresses</td>
<td>2 K</td>
<td>1536</td>
<td>8 K</td>
</tr>
<tr>
<td>IPv4 IGMP groups and multicast routes</td>
<td>1 K</td>
<td>1 K</td>
<td>1 K</td>
</tr>
<tr>
<td>Total IPv4 unicast routes</td>
<td>3 K</td>
<td>2816</td>
<td>0</td>
</tr>
<tr>
<td>- Directly connected IPv4 hosts</td>
<td>2 K</td>
<td>1536</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 7-2 Approximate Feature Resources Allowed by Dual IPv4-IPv6 Templates

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Indirect IPv4 routes</td>
<td>1 K</td>
<td>1280</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 multicast groups</td>
<td>1 K</td>
<td>1152</td>
<td>1 K</td>
</tr>
<tr>
<td>Total IPv6 unicast routes</td>
<td>3 K</td>
<td>2816</td>
<td>0</td>
</tr>
<tr>
<td>Directly connected IPv6 addresses</td>
<td>2 K</td>
<td>1536</td>
<td>0</td>
</tr>
<tr>
<td>Indirect IPv6 unicast routes</td>
<td>1 K</td>
<td>1280</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 policy-based routing ACEs</td>
<td>0</td>
<td>256</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 or MAC QoS ACEs (total)</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>IPv4 or MAC security ACEs (total)</td>
<td>1 K</td>
<td>512</td>
<td>1 K</td>
</tr>
<tr>
<td>IPv6 policy-based routing ACEs²</td>
<td>0</td>
<td>255</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 QoS ACEs</td>
<td>510</td>
<td>510</td>
<td>510</td>
</tr>
<tr>
<td>IPv6 security ACEs</td>
<td>510</td>
<td>510</td>
<td>510</td>
</tr>
</tbody>
</table>

1. Template estimates are based on a switch with 8 routed interfaces and approximately 1000 VLANs.
2. IPv6 policy-based routing is not supported.

Configuring the Switch SDM Template

- Default SDM Template, page 7-3
- SDM Template Configuration Guidelines, page 7-3
- Setting the SDM Template, page 7-4

Default SDM Template

The default template is the default desktop template.

SDM Template Configuration Guidelines

- When you select and configure SDM templates, you must reload the switch for the configuration to take effect.
- Use the `sdm prefer vlan` global configuration command only on switches intended for Layer 2 switching with no routing. When you use the VLAN template, no system resources are reserved for routing entries, and any routing is done through software. This overloads the CPU and severely degrades routing performance.
- Do not use the routing template if you do not have routing enabled on your switch. The `sdm prefer routing` global configuration command prevents other features from using the memory allocated to unicast routing in the routing template.
• If you try to configure IPv6 features without first selecting a dual IPv4 and IPv6 template, a warning message appears.
• Using the dual stack templates results in less TCAM capacity allowed for each resource, so do not use it if you plan to forward only IPv4 traffic.

## Setting the SDM Template

Beginning in privileged EXEC mode, follow these steps to use the SDM template to maximize feature usage:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| Step 2  | sdm prefer {access | default | dual-ipv4-and-ipv6 {default | routing | vlan} | routing | vlan} | Specify the SDM template to be used on the switch: The keywords have these meanings:
  • access—Maximizes system resources for ACLs.
  • default—Gives balance to all functions.
  • dual-ipv4-and-ipv6—Select a template that supports both IPv4 and IPv6 routing.
    • default—Balance IPv4 and IPv6 Layer 2 and Layer 3 functionality.
    • routing—Provide maximum usage for IPv4 and IPv6 routing, including IPv4 policy-based routing.
    • vlan—Provide maximum usage for IPv4 and IPv6 VLANs.
  • routing—Maximizes IPv4 routing on the switch.
  • vlan—Maximizes VLAN configuration on the switch with no routing supported in hardware.
Use the no sdm prefer command to set the switch to the default template. |
| Step 3  | end | Return to privileged EXEC mode. |
| Step 4  | reload | Reload the operating system. |

After the system reboots, you can use the show sdm prefer privileged EXEC command to verify the new template configuration. If you enter the show sdm prefer command before you enter the reload privileged EXEC command, the show sdm prefer command shows the template in use and the template that becomes active after a reload.

This is an example of an output display when you have changed the template and have not reloaded the switch:

```
Switch# show sdm prefer
The current template is "desktop routing" template.
The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses: 3K
  number of igmp groups + multicast routes: 1K
```
Displaying the SDM Templates

Use the `show sdm prefer` privileged EXEC command with no parameters to display the active template.

Use the `show sdm prefer [access | default | dual-ipv4-and-ipv6 {default | vlan | routing} vlan]` privileged EXEC command to display the resource numbers supported by the specified template.

This is an example of output from the `show sdm prefer` command, displaying the template in use.

```
Switch# show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 6K
number of igmp groups + multicast routes: 1K
number of unicast routes: 8K
  number of directly connected hosts: 6K
  number of indirect routes: 2K
number of policy based routing aces: 0
number of qos aces: 512
number of security aces: 1K
```

This is an example of output from the `show sdm prefer routing` command:

```
Switch# show sdm prefer routing
"desktop routing" template:
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 3K
number of igmp groups + multicast routes: 1K
number of unicast routes: 11K
  number of directly connected hosts: 3K
  number of indirect routes: 8K
number of policy based routing aces: 512
```
number of qos aces: 512
number of security aces: 1K

This is an example of output from the `show sdm prefer dual-ipv4-and-ipv6 default` command:

```
Switch# show sdm prefer dual-ipv4-and-ipv6 default
"desktop IPv4 and IPv6 default" template:
The selected template optimizes the resources in the switch to support this level of features for 8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 2K
number of IPV4 IGMP groups + multicast routes: 1K
number of IPV4 unicast routes: 3K
  number of directly-connected IPV4 hosts: 2K
  number of indirect IPV4 routes: 1K
number of IPV6 multicast groups: 1K
number of directly-connected IPV6 addresses: 2K
number of indirect IPV6 unicast routes: 1K
number of IPV4 policy based routing aces: 0
number of IPV4/MAC qos aces: 512
number of IPV4/MAC security aces: 1K
number of IPV6 policy based routing aces: 0
number of IPV6 qos aces: 510
number of IPV6 security aces: 510
```
Configuring Switch-Based Authentication

This chapter describes how to configure switch-based authentication on the Catalyst 3560 switch. This chapter consists of these sections:

- Preventing Unauthorized Access to Your Switch, page 8-1
- Protecting Access to Privileged EXEC Commands, page 8-2
- Controlling Switch Access with TACACS+, page 8-10
- Controlling Switch Access with RADIUS, page 8-18
- Controlling Switch Access with Kerberos, page 8-39
- Configuring the Switch for Local Authentication and Authorization, page 8-43
- Configuring the Switch for Secure Shell, page 8-45
- Configuring the Switch for Secure Socket Layer HTTP, page 8-49
- Configuring the Switch for Secure Copy Protocol, page 8-56

Preventing Unauthorized Access to Your Switch

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 more information, see the “Protecting Access to Privileged EXEC Commands” section on page 8-2.

- 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.
For more information, see the “Configuring Username and Password Pairs” section on page 8-6.

- 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. For more information, see the “Controlling Switch Access with TACACS+” section on page 8-10.

- 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 at this URL:

### Protecting Access to Privileged EXEC Commands

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.

**Note**

For complete syntax and usage information for the commands used in this section, see the *Cisco IOS Security Command Reference, Release 12.2* from the Cisco.com page under **Documentation > Cisco IOS Software > 12.2 Mainline > Command References**.

These sections contain this configuration information:

- Default Password and Privilege Level Configuration, page 8-2
- Setting or Changing a Static Enable Password, page 8-3
- Protecting Enable and Enable Secret Passwords with Encryption, page 8-3
- Disabling Password Recovery, page 8-5
- Setting a Telnet Password for a Terminal Line, page 8-6
- Configuring Username and Password Pairs, page 8-6
- Configuring Multiple Privilege Levels, page 8-8

### Default Password and Privilege Level Configuration

*Table 8-1* 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>
## Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Beginning in privileged EXEC mode, follow these steps to set or change a static enable password:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: enable password password</td>
<td>Define a new password or change an existing password for access to privileged EXEC mode. By default, no password is defined. 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. 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: Enter abc. Enter Ctrl-v. Enter ?123. 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 abc?123 at the password prompt.</td>
</tr>
<tr>
<td>Step 3: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4: show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file. The enable password is not encrypted and can be read in the switch configuration file.</td>
</tr>
</tbody>
</table>

To remove the password, use the **no enable password** global configuration command.

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
```

## Protecting Enable and Enable Secret Passwords with Encryption

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.
Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>enable password [level level] {password</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>service password-encryption</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels. For more information, see the “Configuring Multiple Privilege Levels” section on page 8-8.

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.

To remove a password and level, use the **no enable password [level level]** or **no enable secret [level level]** global configuration command. To disable password encryption, use the **no service password-encryption** global configuration command.
This example shows how to configure the encrypted password $1$FaD0$Xyti5Rkls3LoyxzS8 for privilege level 2:

\[
\text{Switch(config)}# \text{enable secret level 2} 5 \: $1$FaD0$Xyti5Rkls3LoyxzS8
\]

### Disabling 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.

---

**Note**

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. For more information, see the “Recovering from a Lost or Forgotten Password” section on page 48-3.

---

Beginning in privileged EXEC mode, follow these steps to disable password recovery:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 no service password-recovery</td>
<td>Disable password recovery. 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.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show version</td>
<td>Verify the configuration by checking the last few lines of the command output.</td>
</tr>
</tbody>
</table>

To re-enable password recovery, use the `service password-recovery` global configuration command.

**Note**

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.
## Setting a Telnet Password for a Terminal Line

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 now through the command-line interface (CLI).

Beginning in privileged EXEC mode, follow these steps to configure your switch for Telnet access:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Attach a PC or workstation with emulation software to the switch console 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.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>enable password <em>password</em> Enter privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>line vty 0 15 Configure the number of Telnet sessions (lines), and enter 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><strong>Step 5</strong></td>
<td>password <em>password</em> Enter a Telnet password for the line or lines. 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. By default, no password is defined.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show running-config Verify your entries. The password is listed under the command <em>line vty 0 15</em>.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the password, use the `no password` global configuration command.

This example shows how to set the Telnet password to `let45me67in89`:

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

## Configuring 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.
Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>username name [privilege level]</td>
</tr>
<tr>
<td></td>
<td>Enter the username, privilege level, and password for each user.</td>
</tr>
<tr>
<td></td>
<td>• For name, specify the user ID as one word. Spaces and quotation marks are not allowed.</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><strong>Step 3</strong></td>
<td>line console 0</td>
</tr>
<tr>
<td>or</td>
<td>line vty 0 15</td>
</tr>
<tr>
<td></td>
<td>Enter line configuration mode, and configure the console port (line 0) or the VTY lines (line 0 to 15).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>login local</td>
</tr>
<tr>
<td></td>
<td>Enable local password checking at login time. Authentication is based on the username specified in Step 2.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable username authentication for a specific user, use the `no username name` global configuration command. To disable password checking and allow connections without a password, use the `no login` line configuration command.
Configuring Multiple Privilege Levels

By default, the Cisco IOS software has two modes of password security: user EXEC and privileged EXEC. 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.

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.

These sections contain this configuration information:

- Setting the Privilege Level for a Command, page 8-8
- Changing the Default Privilege Level for Lines, page 8-9
- Logging into and Exiting a Privilege Level, page 8-10

Setting the Privilege Level for a Command

Beginning in privileged EXEC mode, follow these steps to set the privilege level for a command mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>privilege mode level level command</code></td>
<td>Set the privilege level for a command.</td>
</tr>
<tr>
<td></td>
<td>• For <code>mode</code>, enter <code>configure</code> for global configuration mode, <code>exec</code> for EXEC mode, <code>interface</code> for interface configuration mode, or <code>line</code> for line configuration mode.</td>
</tr>
<tr>
<td></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></td>
<td>• For <code>command</code>, specify the command to which you want to restrict access.</td>
</tr>
<tr>
<td><code>enable password level level password</code></td>
<td>Specify the enable password for the privilege level.</td>
</tr>
<tr>
<td></td>
<td>• For <code>level</code>, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.</td>
</tr>
<tr>
<td></td>
<td>• For <code>password</code>, 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><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><code>show privilege</code></td>
<td>The first command shows the password and access level configuration.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

These sections contain this configuration information:

- Setting the Privilege Level for a Command, page 8-8
- Changing the Default Privilege Level for Lines, page 8-9
- Logging into and Exiting a Privilege Level, page 8-10
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.

To return to the default privilege for a given command, use the `no privilege mode level level command` global configuration command.

This example shows how to set the `configure` command to privilege level 14 and define `SecretPswd14` as the password users must enter to use level 14 commands:

```
Switch(config)# privilege exec level 14 configure
Switch(config)# enable password level 14 SecretPswd14
```

### Changing the Default Privilege Level for Lines

Beginning in privileged EXEC mode, follow these steps to change the default privilege level for a line:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>line vty line</code></td>
</tr>
<tr>
<td></td>
<td>Select the virtual terminal line on which to restrict access.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>privilege level level</code></td>
</tr>
<tr>
<td></td>
<td>Change the default privilege level for the line.</td>
</tr>
<tr>
<td></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>Step 4</td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>The first command shows the password and access level configuration.</td>
</tr>
<tr>
<td></td>
<td><code>show privilege</code></td>
</tr>
<tr>
<td></td>
<td>The second command shows the privilege level configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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.

To return to the default line privilege level, use the `no privilege level` line configuration command.
Logging into and Exiting a Privilege Level

Beginning in privileged EXEC mode, follow these steps to log in to a specified privilege level and to exit to a specified privilege level:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>enable level</td>
<td>Log in to a specified privilege level. For level, the range is 0 to 15.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>disable level</td>
<td>Exit to a specified privilege level. For level, the range is 0 to 15.</td>
</tr>
</tbody>
</table>

Controlling Switch Access with TACACS+

This section describes how to enable and configure Terminal Access Controller Access Control System Plus (TACACS+), which provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization, accounting (AAA) and can be enabled only through AAA commands.

Note
For complete syntax and usage information for the commands used in this section, see the Cisco IOS Security Command Reference, Release 12.2.

These sections contain this configuration information:
- Understanding TACACS+, page 8-10
- TACACS+ Operation, page 8-12
- Configuring TACACS+, page 8-13
- Displaying the TACACS+ Configuration, page 8-18

Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your switch. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You should have access to and should configure a TACACS+ server before the configuring TACACS+ features on 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—indepedently. 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. A network access server provides connections to a single user, to a network or subnetwork, and to interconnected networks as shown in Figure 8-1.
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.

You need a system running the TACACS+ daemon software to use TACACS+ on your switch.

**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
Configuring TACACS+

This section describes how to configure your switch to support TACACS+. 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. 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.

These sections contain this configuration information:
- Default TACACS+ Configuration, page 8-13
- Identifying the TACACS+ Server Host and Setting the Authentication Key, page 8-13
- Configuring TACACS+ Login Authentication, page 8-14
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 8-16
- Starting TACACS+ Accounting, page 8-17

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

Note

Although TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

Identifying the TACACS+ Server Host and Setting the Authentication Key

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.
Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2** tacacs-server host hostname [port integer] [timeout integer] [key string] | Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them.  
  - For hostname, specify the name or IP address of the host.  
  - (Optional) For port integer, specify a server port number. The default is port 49. The range is 1 to 65535.  
  - (Optional) For timeout integer, specify a time in seconds the switch waits for a response from the daemon before it times out and declares an error. The default is 5 seconds. The range is 1 to 1000 seconds.  
  - (Optional) For key string, specify the encryption key for encrypting and decrypting all traffic between the switch and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful. |
| **Step 3** aaa new-model          | Enable AAA.                                                             |
| **Step 4** aaa group server tacacs+ group-name | (Optional) Define the AAA server-group with a group name.  
  This command puts the switch in a server group subconfiguration mode. |
| **Step 5** server ip-address      | (Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group.  
  Each server in the group must be previously defined in Step 2. |
| **Step 6** end                    | Return to privileged EXEC mode.                                        |
| **Step 7** show tacacs            | Verify your entries.                                                   |
| **Step 8** copy running-config startup-config | (Optional) Save your entries in the configuration file.                 |

To remove the specified TACACS+ server name or address, use the `no tacacs-server host hostname` global configuration command. To remove a server group from the configuration list, use the `no aaa group server tacacs+ group-name` global configuration command. To remove the IP address of a TACACS+ server, use the `no server ip-address` server group subconfiguration command.

### Configuring TACACS+ 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 (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.

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.

Beginning in privileged EXEC mode, follow these steps to configure login authentication:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa new-model</td>
</tr>
</tbody>
</table>
| Step 3  | aaa authentication login \{default | Create a login authentication method list.
| list-name\} method1 [method2...] | - To create a default list that is used when a named list is *not* specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.
- For list-name, specify a character string to name the list you are creating.
- For method1..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Select one of these methods:
- **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the enable password global configuration command.
- **group tacacs+**—Uses TACACS+ authentication. Before you can use this authentication method, you must configure the TACACS+ server. For more information, see the “Identifying the TACACS+ Server Host and Setting the Authentication Key” section on page 8-13.
- **line**—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the password password line configuration command.
- **local**—Use the local username database for authentication. You must enter username information in the database. Use the username password global configuration command.
- **local-case**—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the username name password global configuration command.
- **none**—Do not use any authentication for login.

| Step 4  | line [console | tty | vty] line-number [ending-line-number] | Enter line configuration mode, and configure the lines to which you want to apply the authentication list. |
To disable AAA, use the `no aaa new-model` global configuration command. To disable AAA authentication, use the `no aaa authentication login {default | list-name} method1 [method2...]` global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the `no login authentication {default | list-name}` line configuration command.

**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 12.2* from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

### Configuring 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.

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.

The `aaa authorization exec tacacs+ local` command sets these authorization parameters:

- 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+.

**Note**
Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.
Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa authorization network tacacs+</td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa authorization exec tacacs+</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable authorization, use the `no aaa authorization network | exec method1` global configuration command.

**Starting 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.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa accounting network start-stop tacacs+</td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa accounting exec start-stop tacacs+</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable accounting, use the `no aaa accounting network | exec {start-stop} method1...` global configuration 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.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the `show tacacs` privileged EXEC command.

Controlling Switch Access with RADIUS

This section describes how to enable and configure the RADIUS, which provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through AAA and can be enabled only through AAA commands.

Note

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Security Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

These sections contain this configuration information:

- Understanding RADIUS, page 8-18
- RADIUS Operation, page 8-20
- RADIUS Change of Authorization, page 8-20
- Configuring RADIUS, page 8-26
- Displaying the RADIUS Configuration, page 8-39

Understanding RADIUS

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.
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.

Use RADIUS in these network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors’ access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.

- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma’s security cards to validates users and to grant access to network resources.

- Networks already using RADIUS. You can add a Cisco switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 8-2 on page 8-20.

- 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 9, “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.

RADIUS is not suitable in these 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.
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 these responses from the RADIUS server:
   a. ACCEPT—The user is authenticated.
   b. REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   c. CHALLENGE—A challenge requires additional data from the user.
   d. 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. Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled. 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

RADIUS Change of Authorization

This section provides an overview of the RADIUS interface including available primitives and how they are used during a Change of Authorization (CoA).

- Overview, page 8-21
- Change-of-Authorization Requests, page 8-21
- CoA Request Response Code, page 8-22
Overview

A standard RADIUS interface is typically used in a pulled model where the request originates from a network attached device and the response come from the queried servers. Catalyst switches support the RADIUS Change of Authorization (CoA) extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

Beginning with Cisco IOS Release 12.2(52)SE, the switch supports these per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce

This feature is integrated with the Cisco Secure Access Control Server (ACS) 5.1. For information about ACS:

The RADIUS interface is enabled by default on Catalyst switches. However, some basic configuration is required for these attributes:

- Security and Password—See the “Preventing Unauthorized Access to Your Switch” section in the “Configuring Switch-Based Authentication” chapter in the Catalyst 3750 Switch Software Configuration Guide, Cisco Release 12.2(50)SE.
- Accounting—See the “Starting RADIUS Accounting” section in the “Configuring Switch-Based Authentication” chapter in the Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE.

Change-of-Authorization Requests

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for session identification, host reauthentication, and session termination. The model is comprised of one request (CoA-Request) and two possible response codes:

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA non-acknowledgement (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the switch that acts as a listener.

This section includes these topics:

- CoA Request Response Code
- CoA Request Commands
- Session Reauthentication

RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the switch for session termination.
Table 8-2 shows the IETF attributes are supported for this feature.

**Table 8-2 Supported IETF Attributes**

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>State</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-ID</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
</tr>
<tr>
<td>101</td>
<td>Error-Cause</td>
</tr>
</tbody>
</table>

Table 8-3 shows the possible values for the Error-Cause attribute.

**Table 8-3 Error-Cause Values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Residual Session Context Removed</td>
</tr>
<tr>
<td>202</td>
<td>Invalid EAP Packet (Ignored)</td>
</tr>
<tr>
<td>401</td>
<td>Unsupported Attribute</td>
</tr>
<tr>
<td>402</td>
<td>Missing Attribute</td>
</tr>
<tr>
<td>403</td>
<td>NAS Identification Mismatch</td>
</tr>
<tr>
<td>404</td>
<td>Invalid Request</td>
</tr>
<tr>
<td>405</td>
<td>Unsupported Service</td>
</tr>
<tr>
<td>406</td>
<td>Unsupported Extension</td>
</tr>
<tr>
<td>407</td>
<td>Invalid Attribute Value</td>
</tr>
<tr>
<td>501</td>
<td>Administratively Prohibited</td>
</tr>
<tr>
<td>502</td>
<td>Request Not Routable (Proxy)</td>
</tr>
<tr>
<td>503</td>
<td>Session Context Not Found</td>
</tr>
<tr>
<td>504</td>
<td>Session Context Not Removable</td>
</tr>
<tr>
<td>505</td>
<td>Other Proxy Processing Error</td>
</tr>
<tr>
<td>506</td>
<td>Resources Unavailable</td>
</tr>
<tr>
<td>507</td>
<td>Request Initiated</td>
</tr>
<tr>
<td>508</td>
<td>Multiple Session Selection Unsupported</td>
</tr>
</tbody>
</table>

**Preconditions**

To use the 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.

**CoA Request Response Code**

The CoA Request response code can be used to convey a command to the switch. The supported commands are listed in Table 8-4 on page 8-24.
Session Identification

For disconnect and CoA requests targeted at a particular session, the switch locates the session based on one or more of the following attributes:

- Calling-Station-Id (IETF attribute 31 which contains the host MAC address)
- Audit-Session-Id (Cisco VSA)
- Acct-Session-Id (IETF attribute 44)

Unless all session identification attributes included in the CoA message match the session, the switch returns a Disconnect-NAK or CoA-NAK with the Invalid Attribute Value error-code attribute.

For disconnect and CoA requests targeted to a particular session, any one of these session identifiers can be used:

- Calling-Station-ID (IETF attribute 31, which should contain the MAC address)
- Audit-Session-ID (Cisco vendor-specific attribute)
- Accounting-Session-ID (IETF attribute 44).

If more than one session identification attribute is included in the message, all the attributes must match the session or the switch returns a Disconnect- negative acknowledgement (NAK) or CoA-NAK with the error code Invalid Attribute Value.

The packet format for a CoA Request code as defined in RFC 5176 consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format.

```
  +-----------------+------------------+-
  |     Code        |  Identifier   |            Length             |
  +-----------------+------------------+-
  |                                                               |
  |                         Authenticator                         |
  |                                                               |
  |                                                               |
  +-----------------+------------------+-
  |  Attributes ...  |
  +-----------------+-
```

The attributes field is used to carry Cisco VSAs.

CoA ACK Response Code

If the authorization state is changed successfully, a positive acknowledgement (ACK) is sent. The attributes returned within CoA ACK will vary based on the CoA Request and are discussed in individual CoA Commands.

CoA NAK Response Code

A negative acknowledgement (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. Use `show` commands to verify a successful CoA.
CoA Request Commands

This section includes:

- Session Reauthentication
- Session Termination
- CoA Disconnect-Request
- CoA Request: Disable Host Port
- CoA Request: Bounce-Port

Beginning with Cisco IOS Release 12.2(52)SE, the switch supports the commands shown in Table 8-4.

### Table 8-4  CoA Commands Supported on the Switch

<table>
<thead>
<tr>
<th>Command1</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reauthenticate host</td>
<td>Cisco:Avpair=“subscriber:command=reauthenticate”</td>
</tr>
<tr>
<td>Terminate session</td>
<td>This is a standard disconnect request that does not require a VSA.</td>
</tr>
<tr>
<td>Bounce host port</td>
<td>Cisco:Avpair=“subscriber:command=bounce-host-port”</td>
</tr>
<tr>
<td>Disable host port</td>
<td>Cisco:Avpair=“subscriber:command=disable-host-port”</td>
</tr>
</tbody>
</table>

1. All CoA commands must include the session identifier between the switch and the CoA client.

**Session Reauthentication**

The AAA server typically generates a session reauthentication request when a host with an unknown identity or posture joins the network and is associated with a restricted access authorization profile (such as a guest VLAN). A reauthentication request allows the host to be placed in the appropriate authorization group when its credentials are known.

To initiate session authentication, the AAA server sends a standard CoA-Request message which contains a Cisco vendor-specific attribute (VSA) in this form: `Cisco:Avpair=“subscriber:command=reauthenticate”` and one or more session identification attributes.

The current session state determines the switch response to the message. If the session is currently authenticated by IEEE 802.1x, the switch responds by sending an Extensible Authentication Protocol over LAN (EAPoL) RequestId message to the server.

If the session is currently authenticated by MAC authentication bypass (MAB), the switch sends an access-request to the server, passing the same identity attributes used for the initial successful authentication.

If session authentication is in progress when the switch receives the command, the switch terminates the process, and restarts the authentication sequence, starting with the method configured to be attempted first.

If the session is not yet authorized, or is authorized via guest VLAN, or critical VLAN, or similar policies, the reauthentication message restarts the access control methods, beginning with the method configured to be attempted first. The current authorization of the session is maintained until the reauthentication leads to a different authorization result.
Session Termination

There are three types of CoA requests that can trigger session termination. A CoA Disconnect-Request terminates the session, without disabling the host port. This command causes re-initialization of the authenticator state machine for the specified host, but does not restrict that host’s access to the network.

To restrict a host’s access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to be causing problems on the network, and you need to immediately block network access for the host. When you want to restore network access on the port, re-enable it using a non-RADIUS mechanism.

When a device with no supplicant, such as a printer, needs to acquire a new IP address (for example, after a VLAN change), terminate the session on the host port with port-bounce (temporarily disable and then re-enable the port).

CoA Disconnect-Request

This command is a standard Disconnect-Request. Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “Session Identification” section on page 8-23. If the session cannot be located, the switch returns a Disconnect-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch terminates the session. After the session has been completely removed, the switch returns a Disconnect-ACK.

If the switch fails-over to a standby switch before returning a Disconnect-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the session is not found following re-sending, a Disconnect-ACK is sent with the “Session Context Not Found” error-code attribute.

CoA Request: Disable Host Port

This command is carried in a standard CoA-Request message that has this new VSA:
Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “Session Identification” section on page 8-23. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port and returns a CoA-ACK message.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is restarted on the new active switch.

A Disconnect-Request failure following command re-sending could be the result of either a successful session termination before change-over (if the Disconnect-ACK was not sent) or a session termination by other means (for example, a link failure) that occurred after the original command was issued and before the standby switch became active.

CoA Request: Bounce-Port

This command is carried in a standard CoA-Request message that contains this VSA:
Cisco:Avpair="subscriber:command=bounce-host-port"
Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the “Session Identification” section on page 8-23. If the session cannot be located, the switch returns a CoA-NAK message with the “Session Context Not Found” error-code attribute. If the session is located, the switch disables the hosting port for a period of 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is re-started on the new active switch.

Configuring RADIUS

This section describes how to configure your switch to support RADIUS. 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.

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 (such as TACACS+ or local username lookup), 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.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your switch.

- Default RADIUS Configuration, page 8-26
- Identifying the RADIUS Server Host, page 8-27 (required)
- Configuring RADIUS Login Authentication, page 8-29 (required)
- Defining AAA Server Groups, page 8-31 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 8-33 (optional)
- Starting RADIUS Accounting, page 8-34 (optional)
- Configuring Settings for All RADIUS Servers, page 8-35 (optional)
- Configuring the Switch to Use Vendor-Specific RADIUS Attributes, page 8-35 (optional)
- Configuring the Switch for Vendor-Proprietary RADIUS Server Communication, page 8-37 (optional)
- Configuring CoA on the Switch, page 8-38
- Monitoring and Troubleshooting CoA Functionality, page 8-39
- Configuring RADIUS Server Load Balancing, page 8-39 (optional)

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.
Identifying the 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. 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`. To apply these values on a specific RADIUS server, use the `radius-server host` global configuration command.

**Note**

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 the “Configuring Settings for All RADIUS Servers” section on page 8-35.

You can configure the switch to use AAA server groups to group existing server hosts for authentication. For more information, see the “Defining AAA Server Groups” section on page 8-31.
Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

<table>
<thead>
<tr>
<th>Command</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> radius-server host {hostname</td>
<td>Specify the IP address or hostname of the remote RADIUS server host.</td>
</tr>
<tr>
<td>ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</td>
<td>• (Optional) For auth-port port-number, specify the UDP destination port for authentication requests.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For acct-port port-number, specify the UDP destination port for accounting requests.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For timeout seconds, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For retransmit retries, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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 host 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.</td>
</tr>
<tr>
<td></td>
<td>To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show running-config</td>
<td>Verify your entries.</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>
</tbody>
</table>

To remove the specified RADIUS server, use the no radius-server host hostname | ip-address global configuration command.

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
```

**Note** 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.

### Configuring 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 (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 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.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>aaa new-model</td>
<td>Enable AAA.</td>
</tr>
</tbody>
</table>
### Step 3

**Command**

```
aaa authentication login {default \ list-name} method1 [method2...]
```

**Purpose**

Create a login authentication method list.

- To create a default list that is used when a named list is not specified in the `login authentication` command, use the `default` keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.

- For `list-name`, specify a character string to name the list you are creating.

- For `method1...`, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

Select one of these methods:

- **enable**—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the `enable password` global configuration command.

- **group radius**—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server. For more information, see the “Identifying the RADIUS Server Host” section on page 8-27.

- **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.

- **local**—Use the local username database for authentication. You must enter username information in the database. Use the `username name password` global configuration command.

- **local-case**—Use a case-sensitive local username database for authentication. You must enter username information in the database by using the `username password` global configuration command.

- **none**—Do not use any authentication for login.

### Step 4

**Command**

```
line [console | tty | vty] line-number [ending-line-number]
```

**Purpose**

Enter line configuration mode, and configure the lines to which you want to apply the authentication list.

### Step 5

**Command**

```
login authentication {default | list-name}
```

**Purpose**

Apply 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 6

**Command**

```
end
```

**Purpose**

Return to privileged EXEC mode.

### Step 7

**Command**

```
show running-config
```

**Purpose**

Verify your entries.

### Step 8

**Command**

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

**Purpose**

(Optional) Save your entries in the configuration file.
To disable AAA, use the `no aaa new-model` global configuration command. To disable AAA authentication, use the `no aaa authentication login {default | list-name} method1 [method2...]` global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the `no login authentication {default | list-name}` line configuration command.

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 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

Defining 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. 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.

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.
Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>radius-server host {hostname</td>
<td>Specify the IP address or hostname of the remote RADIUS server host.</td>
</tr>
<tr>
<td></td>
<td>ip-address} [auth-port</td>
<td>• (Optional) For auth-port port-number, specify the UDP destination port for authentication requests.</td>
</tr>
<tr>
<td></td>
<td>port-number] [acct-port</td>
<td>• (Optional) For acct-port port-number, specify the UDP destination port for accounting requests.</td>
</tr>
<tr>
<td></td>
<td>port-number] [timeout seconds]</td>
<td>• (Optional) For timeout seconds, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used.</td>
</tr>
<tr>
<td></td>
<td>[retransmit retries] [key string]</td>
<td>• (Optional) For retransmit retries, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
</tbody>
</table>

Note: The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host 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.

To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa new-model</td>
<td>Enable AAA.</td>
</tr>
<tr>
<td></td>
<td>aaa group server radius group-name</td>
<td>Define the AAA server-group with a group name.</td>
</tr>
<tr>
<td></td>
<td>This command puts the switch in a server group configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>server ip-address</td>
<td>Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group.</td>
</tr>
<tr>
<td></td>
<td>Each server in the group must be previously defined in Step 2.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>
Controlling Switch Access with RADIUS

To remove the specified RADIUS server, use the `no radius-server host hostname | ip-address` global configuration command. To remove a server group from the configuration list, use the `no aaa group server radius group-name` global configuration command. To remove the IP address of a RADIUS server, use the `no server ip-address` server group configuration command.

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
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged 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 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.

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.

**Note**

Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.
Chapter 8  Configuring Switch-Based Authentication

Controlling Switch Access with RADIUS

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2  aaa authorization network radius</td>
<td>Configure the switch for user RADIUS authorization for all network-related service requests.</td>
</tr>
<tr>
<td>Step 3  aaa authorization exec radius</td>
<td>Configure 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>Step 4  end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5  show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6  copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable authorization, use the no aaa authorization {network | exec} method1 global configuration command.

Starting RADIUS 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 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. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2  aaa accounting network start-stop radius</td>
<td>Enable RADIUS accounting for all network-related service requests.</td>
</tr>
<tr>
<td>Step 3  aaa accounting exec start-stop radius</td>
<td>Enable 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>Step 4  end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5  show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6  copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable accounting, use the no aaa accounting {network | exec} {start-stop} method1... global configuration 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 Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the switch and all RADIUS servers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>radius-server key <code>string</code></td>
<td>Specify the shared secret text string used between the switch and all RADIUS servers.</td>
</tr>
<tr>
<td></td>
<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>3</td>
<td>radius-server retransmit <code>retries</code></td>
<td>Specify the number of times the switch sends each RADIUS request to the server before giving up. The default is 3; the range is 1 to 1000.</td>
</tr>
<tr>
<td>4</td>
<td>radius-server timeout <code>seconds</code></td>
<td>Specify the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.</td>
</tr>
<tr>
<td>5</td>
<td>radius-server deadtime <code>minutes</code></td>
<td>Specify the number of minutes a RADIUS server, which is not responding to authentication requests, to be skipped, thus avoiding the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td>show running-config</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting for the retransmit, timeout, and deadtime, use the `no` forms of these commands.

Configuring the Switch to Use 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, 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"

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).”

Beginning in privileged EXEC mode, follow these steps to configure the switch to recognize and use VSAs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>radius-server vsa send [accounting</td>
<td>Enable the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26.</td>
</tr>
<tr>
<td></td>
<td>authentication]</td>
<td>• (Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) Use the authentication keyword to limit the set of recognized vendor-specific attributes to only authentication attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show running-config</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, see the “RADIUS Attributes” appendix in the Cisco IOS Security Configuration Guide, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

### Configuring the Switch for 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.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 radius-server host {hostname</td>
<td>ip-address} non-standard</td>
</tr>
<tr>
<td>Step 3 radius-server key string</td>
<td>Specify 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. 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.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete the vendor-proprietary RADIUS host, use the `no radius-server host \{hostname | ip-address\}` non-standard global configuration command. To disable the key, use the `no radius-server key` global configuration command.

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
```
Configuring CoA on the Switch

Beginning in privileged EXEC mode, follow these steps to configure CoA on a switch. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa server radius dynamic-author</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>client {ip-address</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>server-key [0</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>port port-number</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>auth-type {any</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>ignore session-key</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>ignore server-key</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>authentication command bounce-port ignore</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>authentication command disable-port ignore</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable AAA, use the **no aaa new-model** global configuration command. To disable the AAA server functionality on the switch, use the **no aaa server radius dynamic authorization** global configuration command.
Monitoring and Troubleshooting CoA Functionality

Use these Cisco IOS commands to monitor and troubleshoot CoA functionality on the switch:

- `debug radius`
- `debug aaa coa`
- `debug aaa pod`
- `debug aaa subsys`
- `debug cmdhd [detail | error | events]`
- `show aaa attributes protocol radius`

Configuring RADIUS Server Load Balancing

This feature allows access and authentication requests to be evenly across all RADIUS servers in a server group. For more information, see the “RADIUS Server Load Balancing” chapter of the “Cisco IOS Security Configuration Guide”, Release 12.2:

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the `show running-config` privileged EXEC command.

Controlling Switch Access with Kerberos

This section describes how to enable and configure the Kerberos security system, which authenticates requests for network resources by using a trusted third party. To use this feature, the cryptographic (that is, supports encryption) versions of the switch software must be installed on your switch.

You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information, see the release notes for this release.

These sections contain this information:

- Understanding Kerberos, page 8-40
- Kerberos Operation, page 8-42
- Configuring Kerberos, page 8-43

For Kerberos configuration examples, see the “Kerberos Configuration Examples” section in the “Security Server Protocols” chapter of the Cisco IOS Security Configuration Guide, Release 12.2:

For complete syntax and usage information for the commands used in this section, see the “Kerberos Commands” section in the “Security Server Protocols” chapter of the Cisco IOS Security Command Reference, Release 12.2:

Note

In the Kerberos configuration examples and in the Cisco IOS Security Command Reference, Release 12.2, the trusted third party can be a Catalyst 3560 switch that supports Kerberos, that is configured as a network security server, and that can authenticate users by using the Kerberos protocol.
Understanding Kerberos

Kerberos is a secret-key network authentication protocol, which was developed at the Massachusetts Institute of Technology (MIT). It uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication and authenticates requests for network resources. Kerberos uses the concept of a trusted third party to perform secure verification of users and services. This trusted third party is called the key distribution center (KDC).

Kerberos verifies that users are who they claim to be and the network services that they use are what the services claim to be. To do this, a KDC or trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in user credential caches. The Kerberos server uses the tickets instead of usernames and passwords to authenticate users and network services.

Note

A Kerberos server can be a Catalyst 3560 switch that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

The Kerberos credential scheme uses a process called single logon. This process authenticates a user once and then allows secure authentication (without encrypting another password) wherever that user credential is accepted.

This software release supports Kerberos 5, which allows organizations that are already using Kerberos 5 to use the same Kerberos authentication database on the KDC that they are already using on their other network hosts (such as UNIX servers and PCs).

In this software release, Kerberos supports these network services:

- Telnet
- rlogin
- rsh (Remote Shell Protocol)

Table 8-5 lists the common Kerberos-related terms and definitions:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>A process by which a user or service identifies itself to another service. For example, a client can authenticate to a switch or a switch can authenticate to another switch.</td>
</tr>
<tr>
<td>Authorization</td>
<td>A means by which the switch identifies what privileges the user has in a network or on the switch and what actions the user can perform.</td>
</tr>
<tr>
<td>Credential</td>
<td>A general term that refers to authentication tickets, such as TGTs and service credentials. Kerberos credentials verify the identity of a user or service. If a network service decides to trust the Kerberos server that issued a ticket, it can be used in place of re-entering a username and password. Credentials have a default lifespan of eight hours.</td>
</tr>
</tbody>
</table>
### Table 8-5  Kerberos Terms (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>An authorization level label for Kerberos principals. Most Kerberos principals are of the form <code>user@REALM</code> (for example, <a href="mailto:smith@EXAMPLE.COM">smith@EXAMPLE.COM</a>). A Kerberos principal with a Kerberos instance has the form <code>user/instance@REALM</code> (for example, smith/admin@EXAMPLE.COM). The Kerberos instance can be used to specify the authorization level for the user if authentication is successful. The server of each network service might implement and enforce the authorization mappings of Kerberos instances but is not required to do so.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Kerberos principal and instance names must be in all lowercase characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>KDC(^2)</td>
<td>Key distribution center that consists of a Kerberos server and database program that is running on a network host.</td>
</tr>
<tr>
<td>Kerberized</td>
<td>A term that describes applications and services that have been modified to support the Kerberos credential infrastructure.</td>
</tr>
<tr>
<td>Kerberos realm</td>
<td>A domain consisting of users, hosts, and network services that are registered to a Kerberos server. The Kerberos server is trusted to verify the identity of a user or network service to another user or network service.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Kerberos realm name must be in all uppercase characters.</td>
</tr>
<tr>
<td>Kerberos server</td>
<td>A daemon that is running on a network host. Users and network services register their identity with the Kerberos server. Network services query the Kerberos server to authenticate to other network services.</td>
</tr>
<tr>
<td>KEYTAB(^3)</td>
<td>A password that a network service shares with the KDC. In Kerberos 5 and later Kerberos versions, the network service authenticates an encrypted service credential by using the KEYTAB to decrypt it. In Kerberos versions earlier than Kerberos 5, KEYTAB is referred to as SRVTAB(^4).</td>
</tr>
<tr>
<td>Principal</td>
<td>Also known as a Kerberos identity, this is who you are or what a service is according to the Kerberos server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The Kerberos principal name must be in all lowercase characters.</td>
</tr>
<tr>
<td>Service credential</td>
<td>A credential for a network service. When issued from the KDC, this credential is encrypted with the password shared by the network service and the KDC. The password is also shared with the user TGT.</td>
</tr>
<tr>
<td>SRVTAB</td>
<td>A password that a network service shares with the KDC. In Kerberos 5 or later Kerberos versions, SRVTAB is referred to as KEYTAB.</td>
</tr>
<tr>
<td>TGT</td>
<td>Ticket granting ticket that is a credential that the KDC issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.</td>
</tr>
</tbody>
</table>

1. TGT = ticket granting ticket
2. KDC = key distribution center
3. KEYTAB = key table
4. SRVTAB = server table
Kerberos Operation

A Kerberos server can be a Catalyst 3560 switch that is configured as a network security server and that can authenticate remote users by using the Kerberos protocol. Although you can customize Kerberos in a number of ways, remote users attempting to access network services must pass through three layers of security before they can access network services.

To authenticate to network services by using a Catalyst 3560 switch as a Kerberos server, remote users must follow these steps:

1. Authenticating to a Boundary Switch, page 8-42
2. Obtaining a TGT from a KDC, page 8-42
3. Authenticating to Network Services, page 8-43

Authenticating to a Boundary Switch

This section describes the first layer of security through which a remote user must pass. The user must first authenticate to the boundary switch. This process then occurs:

1. The user opens an un-Kerberized Telnet connection to the boundary switch.
2. The switch prompts the user for a username and password.
3. The switch requests a TGT from the KDC for this user.
4. The KDC sends an encrypted TGT that includes the user identity to the switch.
5. The switch attempts to decrypt the TGT by using the password that the user entered.
   - If the decryption is successful, the user is authenticated to the switch.
   - If the decryption is not successful, the user repeats Step 2 either by re-entering the username and password (noting if Caps Lock or Num Lock is on or off) or by entering a different username and password.

A remote user who initiates a un-Kerberized Telnet session and authenticates to a boundary switch is inside the firewall, but the user must still authenticate directly to the KDC before getting access to the network services. The user must authenticate to the KDC because the TGT that the KDC issues is stored on the switch and cannot be used for additional authentication until the user logs on to the switch.

Obtaining a TGT from a KDC

This section describes the second layer of security through which a remote user must pass. The user must now authenticate to a KDC and obtain a TGT from the KDC to access network services.

Authenticating to Network Services

This section describes the third layer of security through which a remote user must pass. The user with a TGT must now authenticate to the network services in a Kerberos realm.

For instructions about how to authenticate to a network service, see the “Authenticating to Network Services” section in the “Security Server Protocols” chapter of the Cisco IOS Security Configuration Guide, Release 12.2:

Configuring Kerberos

So that remote users can authenticate to network services, you must configure the hosts and the KDC in the Kerberos realm to communicate and mutually authenticate users and network services. To do this, you must identify them to each other. You add entries for the hosts to the Kerberos database on the KDC and add KEYTAB files generated by the KDC to all hosts in the Kerberos realm. You also create entries for the users in the KDC database.

When you add or create entries for the hosts and users, follow these guidelines:

- The Kerberos principal name must be in all lowercase characters.
- The Kerberos instance name must be in all lowercase characters.
- The Kerberos realm name must be in all uppercase characters.

Note

A Kerberos server can be a Catalyst 3560 switch that is configured as a network security server and that can authenticate users by using the Kerberos protocol.

To set up a Kerberos-authenticated server-client system, follow these steps:

- Configure the KDC by using Kerberos commands.
- Configure the switch to use the Kerberos protocol.

For instructions, see the “Kerberos Configuration Task List” section in the “Security Server Protocols” chapter of the Cisco IOS Security Configuration Guide, Release 12.2:

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.

Beginning in privileged EXEC mode, follow these steps to configure the switch for local AAA:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa new-model</td>
</tr>
<tr>
<td></td>
<td>Enable AAA.</td>
</tr>
</tbody>
</table>
To disable AAA, use the `no aaa new-model` global configuration command. To disable authorization, use the `no aaa authorization { network | exec } method` global configuration command.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>aaa authentication login default local</td>
<td>Set the login authentication to use the local username database. The <code>default</code> keyword applies the local user database authentication to all ports.</td>
</tr>
<tr>
<td>4</td>
<td>aaa authorization exec local</td>
<td>Configure user AAA authorization, check the local database, and allow the user to run an EXEC shell.</td>
</tr>
<tr>
<td>5</td>
<td>aaa authorization network local</td>
<td>Configure user AAA authorization for all network-related service requests.</td>
</tr>
<tr>
<td>6</td>
<td>username name [privilege level] [password encryption-type password]</td>
<td>Enter the local database, and establish a username-based authentication system.</td>
</tr>
<tr>
<td></td>
<td>Repeat this command for each user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For <code>name</code>, specify the user ID as one word. Spaces and quotation marks are not allowed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>level</code>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For <code>encryption-type</code>, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For <code>password</code>, 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 <code>username</code> command.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>9</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
**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 12.2*.

---

### Configuring the Switch for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature. To use this feature, you must install the cryptographic (encrypted) software image on your switch. You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information, see the release notes for this release.

These sections contain this information:

- Understanding SSH, page 8-45
- Configuring SSH, page 8-46
- Displaying the SSH Configuration and Status, page 8-49

For SSH configuration examples, see the “SSH Configuration Examples” section in the “Configuring Secure Shell” chapter of the *Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*:


---

**Note**

For complete syntax and usage information for the commands used in this section, see the command reference for this release and the command reference for Cisco IOS Release 12.2:


---

### Understanding SSH

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).

This section consists of these topics:

- SSH Servers, Integrated Clients, and Supported Versions, page 8-45
- Limitations, page 8-46

### SSH Servers, Integrated Clients, and Supported Versions

The SSH feature has an SSH server and an SSH integrated client, which are applications that run on the switch. You can use an SSH client to connect to a switch running the SSH server. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client also works with the SSH server supported in this release and with non-Cisco SSH servers.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.
SSH supports the Data Encryption Standard (DES) encryption algorithm, the Triple DES (3DES) encryption algorithm, and password-based user authentication.

SSH also supports these user authentication methods:

- TACACS+ (for more information, see the “Controlling Switch Access with TACACS+” section on page 8-10)
- RADIUS (for more information, see the “Controlling Switch Access with RADIUS” section on page 8-18)
- Local authentication and authorization (for more information, see the “Configuring the Switch for Local Authentication and Authorization” section on page 8-43)

**Note**
This software release does not support IP Security (IPSec).

### Limitations

These limitations apply to SSH:

- 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 DES (56-bit) and 3DES (168-bit) data encryption software.
- 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.

### Configuring SSH

This section has this configuration information:

- **Configuration Guidelines, page 8-46**
- **Setting Up the Switch to Run SSH, page 8-47** (required)
- **Configuring the SSH Server, page 8-48** (required only if you are configuring the switch as an SSH server)

### Configuration Guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If you get CLI error messages after entering the `crypto key generate rsa` global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the `crypto key generate rsa` command. For more information, see the “Setting Up the Switch to Run SSH” section on page 8-47.
- When generating the RSA key pair, the message `No host name specified` might appear. If it does, you must configure a hostname by using the `hostname` global configuration command.
- When generating the RSA key pair, the message `No domain specified` might appear. If it does, you must configure an IP domain name by using the `ip domain-name` global configuration command.
• When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

**Setting Up the Switch to Run SSH**

Follow these steps to set up your switch to run SSH:

1. Download the cryptographic software image from Cisco.com. This step is required. For more information, see the release notes for this release.

2. Configure a hostname and IP domain name for the switch. Follow this procedure only if you are configuring the switch as an SSH server.

3. Generate an RSA key pair for the switch, which automatically enables SSH. Follow this procedure only if you are configuring the switch as an SSH server.

4. Configure user authentication for local or remote access. This step is required. For more information, see the “Configuring the Switch for Local Authentication and Authorization” section on page 8-43.

Beginning in privileged EXEC mode, follow these steps to configure a hostname and an IP domain name and to generate an RSA key pair. This procedure is required if you are configuring the switch as an SSH server.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 hostname hostname</td>
<td>Configure a hostname for your switch.</td>
</tr>
<tr>
<td>Step 3 ip domain-name domain_name</td>
<td>Configure a host domain for your switch.</td>
</tr>
<tr>
<td>Step 4 crypto key generate rsa</td>
<td>Enable the SSH server for local and remote authentication on the switch and generate an RSA key pair. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show ip ssh</td>
<td>Show the version and configuration information for your SSH server.</td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete the RSA key pair, use the `crypto key zeroize rsa` global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.
## Configuring the SSH Server

Beginning in privileged EXEC mode, follow these steps to configure the SSH server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip ssh version [1</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the switch to run SSH Version 1 or SSH Version 2.</td>
</tr>
<tr>
<td></td>
<td>• 1—Configure the switch to run SSH Version 1.</td>
</tr>
<tr>
<td></td>
<td>• 2—Configure the switch to run SSH Version 2.</td>
</tr>
<tr>
<td></td>
<td>If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip ssh {timeout seconds</td>
</tr>
<tr>
<td></td>
<td>Configure the SSH control parameters:</td>
</tr>
<tr>
<td></td>
<td>• Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the switch uses the default time-out values of the CLI-based sessions.</td>
</tr>
<tr>
<td></td>
<td>• By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After 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>
<tr>
<td><strong>Step 4</strong></td>
<td>line vty line_number [ending_line_number] transport input ssh</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the virtual terminal line settings.</td>
</tr>
<tr>
<td></td>
<td>• Enter 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.</td>
</tr>
<tr>
<td></td>
<td>• Specify that the switch prevent non-SSH Telnet connections. This limits the router to only SSH connections.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show ip ssh</td>
</tr>
<tr>
<td></td>
<td>Show the version and configuration information for your SSH server.</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>show ssh</td>
</tr>
<tr>
<td></td>
<td>Show the status of the SSH server connections on the switch.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default SSH control parameters, use the `no ip ssh {timeout | authentication-retries}` global configuration command.
Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in Table 8-6:

<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 the Switch for Secure Socket Layer HTTP

This section describes how to configure Secure Socket Layer (SSL) version 3.0 support for the HTTP 1.1 server and client. SSL provides server authentication, encryption, and message integrity, as well as HTTP client authentication, to allow secure HTTP communications. To use this feature, the cryptographic (encrypted) software image must be installed on your switch. You must obtain authorization to use this feature and to download the cryptographic software files from Cisco.com. For more information about the crypto image, see the release notes for this release.

These sections contain this information:

- Understanding Secure HTTP Servers and Clients, page 8-50
- Configuring Secure HTTP Servers and Clients, page 8-52
- Displaying Secure HTTP Server and Client Status, page 8-56

For configuration examples and complete syntax and usage information for the commands used in this section, see the “HTTPS - HTTP Server and Client with SSL 3.0” feature description for Cisco IOS Release 12.2(15)T:
Understanding Secure HTTP Servers and Clients

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://.

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 new 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.
If a self-signed certificate has been generated, this information is included in the output of the `show running-config` privileged EXEC command. This is a partial sample output from that command displaying a self-signed certificate.

```
Switch# show running-config
Building configuration...
<output truncated>
crypto pki trustpoint TP-self-signed-3080755072
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3080755072
  revocation-check none
  rsakeypair TP-self-signed-3080755072
 !
crypto ca certificate chain TP-self-signed-3080755072
  certificate self-signed 01
    3082020F 30820208 A0030201 02020101 300D0609 2A864886 F70D101 0450030
    59312F10 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 33303830
    37353530 37323126 30240609 2A864886 F70D0109
<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.

For additional information on Certificate Authorities, see the “Configuring Certification Authority Interoperability” chapter in the *Cisco IOS Security Configuration Guide, Release 12.2* from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

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-ED3-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_RC4_128_MD5—RSA key exchange with RC4 128-bit encryption and MD5 for message digest
3. SSL_RSA_WITH_RC4_128_SHA—RSA key exchange with RC4 128-bit encryption and SHA for message digest
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA—RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest

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.

Configuring Secure HTTP Servers and Clients

These sections contain this configuration information:

- Default SSL Configuration, page 8-52
- SSL Configuration Guidelines, page 8-52
- Configuring a CA Trustpoint, page 8-53
- Configuring the Secure HTTP Server, page 8-54
- Configuring the Secure HTTP Client, page 8-55

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.
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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>hostname hostname</td>
<td>Specify the hostname of the switch (required only if you have not</td>
</tr>
<tr>
<td></td>
<td></td>
<td>previously configured a hostname). The hostname is required for security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>keys and certificates.</td>
</tr>
<tr>
<td></td>
<td>ip domain-name domain-name</td>
<td>Specify the IP domain name of the switch (required only if you have not</td>
</tr>
<tr>
<td></td>
<td></td>
<td>previously configured an IP domain name). The domain name is required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for security keys and certificates.</td>
</tr>
<tr>
<td></td>
<td>crypto key generate rsa</td>
<td>(Optional) Generate an RSA key pair. RSA key pairs are required before</td>
</tr>
<tr>
<td></td>
<td></td>
<td>you can obtain a certificate for the switch. RSA key pairs are generated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>automatically. You can use this command to regenerate the keys, if</td>
</tr>
<tr>
<td></td>
<td></td>
<td>needed.</td>
</tr>
<tr>
<td></td>
<td>crypto ca trustpoint name</td>
<td>Specify a local configuration name for the CA trustpoint and enter CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>trustpoint configuration mode.</td>
</tr>
<tr>
<td></td>
<td>enrollment url url</td>
<td>Specify the URL to which the switch should send certificate requests.</td>
</tr>
<tr>
<td></td>
<td>enrollment http-proxy host-name port-number</td>
<td>(Optional) Configure the switch to obtain certificates from the CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>through an HTTP proxy server.</td>
</tr>
<tr>
<td></td>
<td>crl query url</td>
<td>Configure the switch to request a certificate revocation list (CRL) to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ensure that the certificate of the peer has not been revoked.</td>
</tr>
<tr>
<td></td>
<td>primary</td>
<td>(Optional) Specify that the trustpoint should be used as the primary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(default) trustpoint for CA requests.</td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td>Exit CA trustpoint configuration mode and return to global configuration</td>
</tr>
<tr>
<td></td>
<td>crypto ca authentication name</td>
<td>Authenticate the CA by getting the public key of the CA. Use the same</td>
</tr>
<tr>
<td></td>
<td></td>
<td>name used in Step 5.</td>
</tr>
<tr>
<td></td>
<td>crypto ca enroll name</td>
<td>Obtain the certificate from the specified CA trustpoint. This command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>requests a signed certificate for each RSA key pair.</td>
</tr>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>show crypto ca trustpoints</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no crypto ca trustpoint name` global configuration command to delete all identity information and certificates associated with the CA.
Configuring the Secure HTTP Server

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.

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **show ip http server status**  
(Optional) Display 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:  
HTTP secure server capability: Present  
or  
HTTP secure server capability: Not present |
| **Step 2** | **configure terminal**  
Enter global configuration mode. |
| **Step 3** | **ip http secure-server**  
Enable the HTTPS server if it has been disabled. The HTTPS server is enabled by default. |
| **Step 4** | **ip http secure-port port-number**  
(Optional) Specify 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]}}  
(Optional) Specify 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**  
(Optional) Configure 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**  
Specify 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. |
| **Step 8** | **ip http path path-name**  
(Optional) Set 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). |
| **Step 9** | **ip http access-class access-list-number**  
(Optional) Specify an access list to use to allow access to the HTTP server. |
| **Step 10** | **ip http max-connections value**  
(Optional) Set the maximum number of concurrent connections that are allowed to the HTTP server. The range is 1 to 16; the default value is 5. |
Configuring the Switch for Secure Socket Layer HTTP

To disable the standard HTTP server, use the `no ip http server` global configuration command. To disable the secure HTTP server, use the `no ip http secure-server` command. Use the `no ip http secure-port` and the `no ip http secure-ciphersuite` commands to return to the default settings. Use the `no ip http secure-client-auth` command to remove the requirement for client authentication.

To verify the secure HTTP connection by using a Web browser, enter `https://URL`, where the URL is the IP address or hostname of the server switch. If you configure a port other than the default port, you must also specify the port number after the URL. For example:

- `https://209.165.129:1026`
- `https://host.domain.com:1026`

### Configuring the Secure HTTP Client

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.

Beginning in privileged EXEC mode, follow these steps to configure a secure HTTP client:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong></td>
<td><code>ip http timeout-policy idle seconds life seconds requests value</code></td>
</tr>
<tr>
<td>Optional) Specify how long a connection to the HTTP server can remain open under the defined circumstances:</td>
<td></td>
</tr>
<tr>
<td>• <code>idle</code>—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).</td>
<td></td>
</tr>
<tr>
<td>• <code>life</code>—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.</td>
<td></td>
</tr>
<tr>
<td>• <code>requests</code>—the maximum number of requests processed on a persistent connection. The maximum value is 86400. The default is 1.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>show ip http server secure status</code></td>
</tr>
<tr>
<td>Display the status of the HTTP secure server to verify the configuration.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
<tr>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

Use the `no ip http server` global configuration command to disable the standard HTTP server. Use the `no ip http secure-server` global configuration command to disable the secure HTTP server. Use the `no ip http secure-port` and the `no ip http secure-ciphersuite` global configuration commands to return to the default settings. Use the `no ip http secure-client-auth` global configuration command to remove the requirement for client authentication.

To verify the secure HTTP connection by using a Web browser, enter `https://URL`, where the URL is the IP address or hostname of the server switch. If you configure a port other than the default port, you must also specify the port number after the URL. For example:

- `https://209.165.129:1026`
- `https://host.domain.com:1026`

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ip http client secure-trustpoint name</code></td>
</tr>
<tr>
<td>(Optional) Specify the CA trustpoint to be used if the remote HTTP server requests client authentication. Using this command assumes that you have already configured a CA trustpoint by using the previous procedure. The command is optional if client authentication is not needed or if a primary trustpoint has been configured.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip http client secure-ciphersuite</code></td>
</tr>
<tr>
<td>(Optional) Specify the CipherSuites (encryption algorithms) to be used for encryption over the HTTPS connection. If you do not have a reason to specify a particular CipherSuite, you should allow the server and client to negotiate a CipherSuite that they both support. This is the default.</td>
<td></td>
</tr>
</tbody>
</table>
Step 4
end
Return to privileged EXEC mode.

Step 5
show ip http client secure status
Display the status of the HTTP secure server to verify the configuration.

Step 6
copy running-config startup-config
(Optional) Save your entries in the configuration file.

Use the no ip http client secure-trustpoint name to remove a client trustpoint configuration. Use the no ip http client secure-ciphersuite to remove a previously configured CipherSuite specification for the client.

Displaying Secure HTTP Server and Client Status

To display the SSL secure server and client status, use the privileged EXEC commands in Table 8-7:

<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>

Configuring the Switch for Secure Copy Protocol

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.
Information About Secure Copy

To configure the Secure Copy feature, you should understand these concepts.

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 router can determine whether the user has the correct privilege level.

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.

IEEE 802.1x port-based authentication prevents unauthorized devices (clients) from gaining access to the network. The switch command reference and the “RADIUS Commands” section in the Cisco IOS Security Command Reference, Release 12.2, have command syntax and usage information.

This chapter includes these sections:
- Understanding IEEE 802.1x Port-Based Authentication, page 10-1
- Configuring 802.1x Authentication, page 10-33
- Displaying 802.1x Statistics and Status, page 10-69

Understanding IEEE 802.1x Port-Based Authentication

The standard defines a client-server-based access control and authentication protocol to prevent unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any switch or LAN services.

Until the client is authenticated, IEEE 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, normal traffic passes through the port.

- Device Roles, page 10-2
- Authentication Process, page 10-3
- Authentication Initiation and Message Exchange, page 10-5
- Authentication Manager, page 10-7
- Ports in Authorized and Unauthorized States, page 10-10
- 802.1x Host Mode, page 10-11
- Multidomain Authentication, page 10-12
- 802.1x Multiple Authentication Mode, page 10-13
- MAC Move, page 10-13
- MAC Replace, page 10-14
- 802.1x Accounting, page 10-14
Device Roles

Device roles with 802.1x port-based authentication:

Figure 10-1   802.1x Device Roles
• **Client**—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the 802.1x standard.)

**Note** To resolve Windows XP network connectivity and 802.1x authentication issues, read the Microsoft Knowledge Base article:  
http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

• **Authentication server**—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the RADIUS security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server. It is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

• **Switch** (edge switch or wireless access point)—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. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server. (The switch is the *authenticator* in the 802.1x standard.)

When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped, and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server’s frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

The devices that can act as intermediaries include the Catalyst 3750-E, Catalyst 3560-E, Catalyst 3750, Catalyst 3560, Catalyst 3550, Catalyst 2975, Catalyst 2970, Catalyst 2960, Catalyst 2955, Catalyst 2950, Catalyst 2940 switches, or a wireless access point. These devices must be running software that supports the RADIUS client and 802.1x authentication.

**Authentication Process**

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.

Figure 10-2 shows the authentication process.

*Figure 10-2 Authentication Flowchart*

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.

If Multidomain authentication (MDA) is enabled on a port, this flow can be used with some exceptions that are applicable to voice authorization. For more information on MDA, see the “Multidomain Authentication” section on page 10-12.

**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` or `dot1x 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 boot up, 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. For more information, see the “Ports in Authorized and Unauthorized States” section on page 10-10.

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. For more information, see the “Ports in Authorized and Unauthorized States” section on page 10-10.

The specific exchange of EAP frames depends on the authentication method being used. Figure 10-3 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 stops 802.1x authentication.

Figure 10-4 shows the message exchange during MAC authentication bypass.
Chapter 10 Configuring IEEE 802.1x Port-Based Authentication

Understanding IEEE 802.1x Port-Based Authentication

Authentication Manager

In Cisco IOS Release 12.2(46)SE and earlier, you could not use the same authorization methods, including CLI commands and messages, on this switch and also on other network devices, such as a Catalyst 6000. You had to use separate authentication configurations. Cisco IOS Release 12.2(50)SE and later supports the same authorization methods on all Catalyst switches in a network.

Cisco IOS Release 12.2(55)SE supports filtering verbose system messages from the authentication manager. For details, see the “Authentication Manager CLI Commands” section on page 10-9.

- Port-Based Authentication Methods, page 10-7
- Per-User ACLs and Filter-Ids, page 10-8
- Authentication Manager CLI Commands, page 10-9

Port-Based Authentication Methods

Table 10-1 lists the authentication methods supported in these host modes:
- Single host–Only one data or voice host (client) can be authenticated on a port.
- Multiple host–Multiple data hosts can be authenticated on the same port. (If a port becomes unauthorized in multiple-host mode, the switch denies network access to all of the attached clients.)
- Multidomain authentication (MDA) –Both a data device and voice device can be authenticated on the same switch port. The port is divided into a data domain and a voice domain.
- Multiple authentication–Multiple hosts can authenticate on the data VLAN. This mode also allows one client on the VLAN if a voice VLAN is configured.

Table 10-1  802.1x Features

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Mode</th>
<th>Single Host</th>
<th>Multiple Host</th>
<th>MDA¹</th>
<th>Multiple Authentication²</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x</td>
<td></td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>Per-user ACL³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL²</td>
<td>Filter-Id attribute³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-Id attribute³</td>
<td>Downloadable ACL³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloadable ACL³</td>
<td>Downloadable ACL³</td>
<td>Downloadable ACL³</td>
<td>Redirect URL³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Redirect URL³</td>
<td>Redirect URL³</td>
<td>Redirect URL³</td>
<td></td>
</tr>
<tr>
<td>MAC authentication bypass</td>
<td></td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>VLAN assignment</td>
<td>Per-user ACL³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Per-user ACL</td>
<td>Per-user ACL</td>
<td>Per-user ACL²</td>
<td>Filter-Id attribute³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Filter-ID attribute</td>
<td>Filter-ID attribute</td>
<td>Filter-Id attribute³</td>
<td>Downloadable ACL³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloadable ACL³</td>
<td>Downloadable ACL³</td>
<td>Downloadable ACL³</td>
<td>Redirect URL³</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Redirect URL³</td>
<td>Redirect URL³</td>
<td>Redirect URL³</td>
<td></td>
</tr>
<tr>
<td>Standalone web authentication²</td>
<td>Proxy ACL, Filter-Id attribute, downloadable ACL²</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Understanding IEEE 802.1x Port-Based Authentication

Chapter 10  Configuring IEEE 802.1x Port-Based Authentication

Table 10-1  802.1x Features (continued)

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Mode</th>
<th>Single Host</th>
<th>Multiple Host</th>
<th>MDA1</th>
<th>Multiple Authentication2</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC Layer 2 IP validation</td>
<td></td>
<td>Filter-Id attribute3</td>
<td>Filter-Id attribute3</td>
<td>Filter-Id attribute3</td>
<td>Filter-Id attribute3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
<tr>
<td>Web authentication as fallback method5</td>
<td></td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
<td>Proxy ACL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Filter-Id attribute3</td>
<td>Filter-Id attribute3</td>
<td>Filter-Id attribute3</td>
<td>Filter-Id attribute3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
<td>Downloadable ACL</td>
</tr>
</tbody>
</table>

1. MDA = Multidomain authentication.
2. Also referred to as multiauth.
4. Supported in Cisco IOS Release 12.2(50)SE and later.
5. For clients that do not support 802.1x authentication.

Per-User ACLs and Filter-Ids

In releases earlier than Cisco IOS Release 12.2(50)SE, per-user ACLs and filter IDs were only supported in single-host mode. In Cisco IOS Release 12.2(50), support was added for MDA- and multiauth-enabled ports. In 12.2(52)SE and later, support was added for ports in multihost mode.

In releases earlier than Cisco IOS Release 12.2(50)SE, an ACL configured on the switch is not compatible with an ACL configured on another device running Cisco IOS software, such as a Catalyst 6000 switch.

In Cisco IOS Release 12.2(50)SE or later, the ACLs configured on the switch are compatible with other devices running the Cisco IOS release.

You can only set any as the source in the ACL.

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 multiauth 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.
AuthenticManager 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. However, the dot1x system-authentication control global configuration command only globally enables or disables 802.1x authentication.

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.

<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 dot1x critical (interface configuration) dot1x guest-vlan6</td>
<td>Enable the restricted VLAN on a port. Enable the inaccessible-authentication-bypass feature. Specify an active VLAN as an guest VLAN.</td>
</tr>
<tr>
<td>authentication fallback</td>
<td>fallback-profile</td>
<td>dot1x fallback fallback-profile</td>
</tr>
<tr>
<td>authentication host-mode</td>
<td>multi-auth</td>
<td>multi-domain</td>
</tr>
<tr>
<td>authentication order</td>
<td>mab</td>
<td>Provides the flexibility to define the order of authentication methods to be used.</td>
</tr>
<tr>
<td>authentication periodic</td>
<td></td>
<td>dot1x reauthentication</td>
</tr>
<tr>
<td>authentication port-control</td>
<td>force-authorized</td>
<td>force-unauthorized</td>
</tr>
</tbody>
</table>
Understanding IEEE 802.1x Port-Based Authentication

Beginning with Cisco IOS Release 12.2(55)SE, you can filter 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.

For more information, see the command reference for this release.

### 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.

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** or **dot1x 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.

---

### Table 10-2 Authentication Manager Commands and Earlier 802.1x Commands (continued)

<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 timer</td>
<td>dot1x timeout</td>
<td>Set the timers.</td>
</tr>
<tr>
<td>authentication violation { protect</td>
<td>restrict</td>
<td>shutdown }</td>
</tr>
</tbody>
</table>

---

Table 10-2 Authentication Manager Commands and Earlier 802.1x Commands (continued)
Chapter 10      Configuring IEEE 802.1x Port-Based Authentication

Understanding IEEE 802.1x Port-Based Authentication

- **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 (see Figure 10-1 on page 10-2), 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. Figure 10-5 on page 10-11 shows 802.1x port-based authentication in a wireless LAN. 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.

With the multiple-hosts mode enabled, you can use 802.1x authentication to authenticate the port and port security to manage network access for all MAC addresses, including that of the client.

**Figure 10-5  Multiple Host Mode Example**
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. For more information, see the “Multidomain Authentication” section on page 10-12.

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.

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:

- To configure a switch port for MDA, see the “Configuring the Host Mode” section on page 10-44.
- You must configure the voice VLAN for the IP phone when the host mode is set to multidomain. For more information, see Chapter 13, “Configuring VLANs.”
- 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 802.1x authentication. For more information, see the “MAC Authentication Bypass” section on page 10-37.
- 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 changes from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone 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-host or multiple-host mode to multidomain mode.
- Switching a port host mode from multidomain to single-host or multiple-hosts mode removes all authorized devices from the port.
- If a data domain is authorized first and placed in the guest VLAN, non-802.1x-capable voice devices need their packets tagged on the voice VLAN to trigger authentication. The phone need not need to send tagged traffic. (The same is true for an 802.1x-capable phone.)
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 port voice and data VLANs. You can use only one device on the port to enforce per-user ACLs.

For more information, see the “Configuring the Host Mode” section on page 10-44.

### 802.1x Multiple Authentication Mode

Multiple-authentication (multiauth) mode allows multiple authenticated clients on the data VLAN. Each host is individually authenticated. If a voice VLAN is configured, this mode also allows one client on the VLAN. (If the port detects any additional voice clients, they are discarded from the port, but no violation errors occur.)

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.

There is no limit to the number of data hosts can authenticate on a multiauth port. However, only one voice device is allowed if the voice VLAN is configured. Since there is no host limit defined violation will not be trigger, if a second voice is seen we silently discard it but do not trigger violation.

For MDA functionality on the voice VLAN, multiple-authentication mode assigns authenticated devices to either a data or a voice VLAN, depending on the VSAs received from the authentication server.

---

**Note**

When a port is in multiple-authentication mode, the guest VLAN and the authentication-failed VLAN features do not activate.

For more information about critical authentication mode and the critical VLAN, see the “802.1x Authentication with Inaccessible Authentication Bypass” section on page 10-23.

For more information about configuring multiauth mode on a port, see the “Configuring the Host Mode” section on page 10-44.

### 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.)

Beginning with Cisco IOS Release 12.2(55)SE, MAC move can be configured in all host modes, along with port security.
Understanding IEEE 802.1x Port-Based Authentication

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. Port security behavior remains the same when you configure MAC move.

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.

For more information see the “Enabling MAC Move” section on page 10-51.

**MAC Replace**

Beginning with Cisco IOS Release 12.2(55)SE, 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.

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.

For more information see the “Enabling MAC Replace” section on page 10-51.

**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.
Understand IEEE 802.1x Port-Based Authentication

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

Table 10-3 lists the AV pairs and when they are sent are sent by the switch:

<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</td>
<td>Always</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[44]</td>
<td>Acct-Session-ID</td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<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>

1. The Framed-IP-Address AV pair is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

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 12.2*:

For more information about AV pairs, see RFC 3580, “802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.”

### 802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. You use an alternate authentication such as MAC authentication bypass or web authentication for the devices that do not support 802.1x functionality.

This feature only works if the supplicant on the client supports a query with the NOTIFY EAP notification packet. The client must respond within the 802.1x timeout value.

For information on configuring the switch for the 802.1x readiness check, see the “Configuring 802.1x Readiness Check” section on page 10-37.

### 802.1x Authentication with VLAN Assignment

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.

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. For more information, see the “Multidomain Authentication” section on page 10-12.

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.

- 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.

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, VLAN ID, or VLAN-Group
  – [83] Tunnel-Preference

Attribute [64] must contain the value VLAN (type 13). Attribute [65] must contain the value 802 (type 6). Attribute [81] specifies the VLAN name or VLAN ID assigned to the 802.1x-authenticated user.

For examples of tunnel attributes, see the “Configuring the Switch to Use Vendor-Specific RADIUS Attributes” section on page 8-35.

### Using 802.1x Authentication with Per-User ACLs

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.

You can configure router ACLs and input port ACLs on the same switch. However, a port ACL takes precedence over a router ACL. If you apply input port ACL to an interface that belongs to a VLAN, the port ACL takes precedence over an input router ACL applied to the VLAN interface. Incoming packets received on the port to which a port ACL is applied are filtered by the port ACL. Incoming routed packets
received on other ports are filtered by the router ACL. Outgoing routed packets are filtered by the router 
ACL. To avoid configuration conflicts, you should carefully plan the user profiles stored on the RADIUS 
server.

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. For 
more information, see Chapter 34, “Configuring Network Security with ACLs.”

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. 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).

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.

For examples of vendor-specific attributes, see the “Configuring the Switch to Use Vendor-Specific 
RADIUS Attributes” section on page 8-35. For more information about configuring ACLs, see 
Chapter 34, “Configuring Network Security with ACLs.”

**Note**
Per-user ACLs are supported only in single-host mode.

To configure per-user ACLs, you need to perform these tasks:

- 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.
- Configure the 802.1x port for single-host mode.

For more configuration information, see the “Authentication Manager” section on page 10-7.

### 802.1x Authentication with Downloadable ACLs and Redirect URLs

You can download ACLs and redirect URLs from a RADIUS server to the switch during 802.1x 
authentication or MAC authentication bypass of the host. You can also download ACLs during web 
authentication.

**Note**
A downloadable ACL is also referred to as a dACL.

If more than one host is authenticated and the host is in single-host, MDA, or multiple-authentication 
mode, the switch changes the source address of the ACL to the host IP address.
You can apply the ACLs and redirect URLs to all the devices connected to the 802.1x-enabled port.

If no ACLs are downloaded during 802.1x authentication, the switch applies the static default ACL on the port to the host. On a voice VLAN port configured in multi-auth or MDA mode, the switch applies the ACL only to the phone as part of the authorization policies.

Beginning with Cisco IOS Release 12.2(55)SE, if there is no static ACL on a port, a dynamic auth-default ACL is created, and policies are enforced before dACLs are downloaded and applied.

The auth-default-ACL does not appear in the running configuration.

The auth-default ACL is created when at least one host with an authorization policy is detected on the port. The auth-default ACL is removed from the port when the last authenticated session ends. You can configure the auth-default ACL by using the `ip access-list extended auth-default-acl` global configuration command.

The auth-default-ACL does not support Cisco Discovery Protocol (CDP) bypass in the single host mode. You must configure a static ACL on the interface to support CDP bypass.

The 802.1x and MAB authentication methods support two authentication modes, *open* and *closed*. If there is no static ACL on a port in *closed* authentication mode:

- An auth-default-ACL is created.
- The auth-default-ACL allows only DHCP traffic until policies are enforced.
- When the first host authenticates, the authorization policy is applied without IP address insertion.
- When a second host is detected, the policies for the first host are refreshed, and policies for the first and subsequent sessions are enforced with IP address insertion.

If there is no static ACL on a port in *open* authentication mode:

- An auth-default-ACL-OPEN is created and allows all traffic.
- Policies are enforced with IP address insertion to prevent security breaches.
- Web authentication is subject to the auth-default-ACL-OPEN.

To control access for hosts with no authorization policy, you can configure a directive. The supported values for the directive are *open* and *default*. When you configure the *open* directive, all traffic is allowed. The *default* directive subjects traffic to the access provided by the port. You can configure the directive either in the user profile on the AAA server or on the switch. To configure the directive on the AAA server, use the `authz-directive =<open/default>` global command. To configure the directive on the switch, use the `epm access-control open` global configuration command.

The default value of the directive is *default*.

If a host falls back to web authentication on a port without a configured ACL:

- If the port is in open authentication mode, the auth-default-ACL-OPEN is created.
- If the port is in closed authentication mode, the auth-default-ACL is created.

The access control entries (ACEs) in the fallback ACL are converted to per-user entries. If the configured fallback profile does not include a fallback ACL, the host is subject to the auth-default-ACL associated with the port.
If you use a custom logo with web authentication and it is stored on an external server, the port ACL must allow access to the external server before authentication. You must either configure a static port ACL or change the auth-default-ACL to provide appropriate access to the external server.

**Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL**

The switch uses these cisco-av-pair VSAs:

- **url-redirect** is the HTTP or HTTPS URL.
- **url-redirect-acl** is the switch ACL name or number.

The switch uses the CiscoSecure-Defined-ACL attribute value pair to intercept an HTTP or HTTPS request from the end point device. The switch then forwards the client web browser to the specified redirect address. The url-redirect attribute value pair on the Cisco Secure ACS contains the URL to which the web browser is redirected. The url-redirect-acl attribute value pair contains the name or number of an ACL that specifies the HTTP or HTTPS traffic to redirect.

Note

- Traffic that matches a permit ACE in the ACL is redirected.
- Define the URL redirect ACL and the default port ACL on the switch.

If a redirect URL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

**Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs**

You can set the CiscoSecure-Defined-ACL Attribute-Value pair on the Cisco Secure ACS with the RADIUS cisco-av-pair vendor-specific attributes (VSAs). This pair specifies the names of the downloadable ACLs on the Cisco Secure ACS with the #ACL#-IP-name-number attribute.

- The **name** is the ACL name.
- The **number** is the version number (for example, 3f783768).

If a downloadable ACL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host-access-policy to the switch, it applies the policy to traffic from the host connected to a switch port. If the policy does not apply, the switch applies the default ACL. If the Cisco Secure ACS sends the switch a downloadable ACL, this ACL takes precedence over the default ACL that is configured on the switch port. However, if the switch receives an host access policy from the Cisco Secure ACS but the default ACL is not configured, the authorization failure is declared.

For configuration details, see the “Authentication Manager” section on page 10-7 and the “Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs” section on page 10-63.

**VLAN ID-based MAC Authentication**

You can use VLAN ID-based MAC authentication if you wish to authenticate hosts based on a static VLAN ID instead of a downloadable VLAN. When you have a static VLAN policy configured on your switch, VLAN information is sent to an IAS (Microsoft) RADIUS server along with the MAC address
of each host for authentication. The VLAN ID configured on the connected port is used for MAC authentication. By using VLAN ID-based MAC authentication with an IAS server, you can have a fixed number of VLANs in the network.

The feature also limits the number of VLANs monitored and handled by STP. The network can be managed as a fixed VLAN.

**Note**

This feature is not supported on Cisco ACS Server. (The ACS server ignores the sent VLAN-IDs for new hosts and only authenticates based on the MAC address.)

For configuration information, see the “Configuring VLAN ID-based MAC Authentication” section on page 10-66. Additional configuration is similar MAC authentication bypass, as described in the “Configuring MAC Authentication Bypass” section on page 10-59.

### 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 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 port is automatically set to multi-host mode.

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 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 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.

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 `dot1x guest-vlan supplicant` global 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.

**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.
Chapter 10      Configuring IEEE 802.1x Port-Based Authentication

Understanding IEEE 802.1x Port-Based Authentication

Guest VLANs are supported on 802.1x ports in single-host or multiple-hosts mode.

You can configure any active VLAN except an RSPAN VLAN, a private VLAN, or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

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 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. For more information, see the “802.1x Authentication with MAC Authentication Bypass” section on page 10-27.

For more information, see the “Configuring a Guest VLAN” section on page 10-53.

---

**802.1x Authentication with Restricted VLAN**

You can configure a restricted VLAN (also referred to as an **authentication failed 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. 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 only on 802.1x ports in single-host mode and on Layer 2 ports. You can configure any active VLAN except an RSPAN VLAN, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

This feature works with port security. As soon as the port is authorized, a MAC address is provided to port security. If port security does not permit the MAC address or if the maximum secure address count is reached, the port becomes unauthorized and error disabled.

Other port security features such as dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.

For more information, see the “Configuring a Restricted VLAN” section on page 10-54.

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.

Support on Multiple-Authentication Ports

To support inaccessible bypass on multiple-authentication (multiauth) ports, you can use the authentication event server dead action reinitialize vlan vlan-id. 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.

The authentication event server dead action reinitialize vlan vlan-id interface configuration command is supported on all host modes.

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 in 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. For more information, see the command reference for this release and the “Configuring Inaccessible Authentication Bypass and Critical Voice VLAN” section on page 10-56.

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 802.1x 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 in 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.
- Private VLAN—You can configure inaccessible authentication bypass on a private VLAN host port. The access VLAN must be a secondary private VLAN.
- 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 access control server (ACS), the phone is put into the voice domain. If the ACS 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.
Chapter 10 Configuring IEEE 802.1x Port-Based Authentication

Understanding IEEE 802.1x Port-Based Authentication

With this release, you can enter the `authentication event server dead action authorize voice` interface configuration command to configure the critical voice VLAN feature. When the ACS 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 CDP (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 is 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 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 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 802.1x authentication is enabled on a voice VLAN port, the switch drops packets from unrecognized IP phones more than one hop away.

When 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

**Note**

If you enable 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.

For more information about voice VLANS, see Chapter 15, “Configuring Voice VLAN.”

### 802.1x Authentication with Port Security

You can configure an 802.1x port with port security in either single-host or multiple-hosts mode. (You also must configure port security on the port by using the `switchport port-security` interface configuration command.) When you enable port security and 802.1x authentication on a port, 802.1x 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 an 802.1x port.
These are some examples of the interaction between 802.1x authentication and port security on the switch:

- When a client is authenticated, and the port security table is not full, the client MAC address is added to the port security list of secure hosts. The port then proceeds to come up normally.
- When a client is authenticated and manually configured for port security, it is guaranteed an entry in the secure host table (unless port security static aging has been enabled).
- A security violation occurs if the client is authenticated, but the port security table is full. This can happen if the maximum number of secure hosts has been statically configured or if the client ages out of the secure host table. If the client address is aged, its place in the secure host table can be taken by another host.
- If the security violation is caused by the first authenticated host, the port becomes error-disabled and immediately shuts down.
- The port security violation modes determine the action for security violations. For more information, see the “Security Violations” section on page 25-11.

- When you manually remove an 802.1x client address from the port security table by using the `no switchport port-security mac-address mac-address` interface configuration command, you should re-authenticate the 802.1x client by using the `dot1x re-authenticate interface interface-id` privileged EXEC command.
- When an 802.1x client logs off, the port changes to an unauthenticated state, and all dynamic entries in the secure host table are cleared, including the entry for the client. Normal authentication then takes place.
- If the port is administratively shut down, the port becomes unauthenticated, and all dynamic entries are removed from the secure host table.
- Port security and a voice VLAN can be configured simultaneously on an 802.1x port that is in either single-host or multiple-hosts mode. Port security applies to both the voice VLAN identifier (VVID) and the port VLAN identifier (PVID).
- You can configure the `authentication violation` or `dot1x violation-mode` interface configuration command so that a port shuts down, generates a syslog error, or discards packets from a new device when it connects to an 802.1x-enabled port or when the maximum number of allowed devices have been authenticated. For more information see the “Maximum Number of Allowed Devices Per Port” section on page 10-37 and the command reference for this release.

For more information about enabling port security on your switch, see the “Configuring Port Security” section on page 25-9.

**802.1x Authentication with Wake-on-LAN**

The 802.1x authentication with the wake-on-LAN (WoL) feature allows dormant PCs to be powered when the switch receives a specific Ethernet frame, known as the *magic packet*. You can use this feature in environments where administrators need to connect to systems that have been powered down.

When a host that uses WoL is attached through an 802.1x port and the host powers off, the 802.1x port becomes unauthorized. The port can only receive and send EAPOL packets, and WoL magic packets cannot reach the host. When the PC is powered off, it is not authorized, and the switch port is not opened.

When the switch uses 802.1x authentication with WoL, the switch forwards traffic to unauthorized 802.1x ports, including magic packets. While the port is unauthorized, the switch continues to block ingress traffic other than EAPOL packets. The host can receive packets but cannot send packets to other devices in the network.
Understanding IEEE 802.1x Port-Based Authentication

Note

If PortFast is not enabled on the port, the port is forced to the bidirectional state.

When you configure a port as unidirectional by using the `authentication control-direction in` or `dot1x control-direction in` interface configuration command, the port changes to the spanning-tree forwarding state. The port can send packets to the host but cannot receive packets from the host.

When you configure a port as bidirectional by using the `authentication control-direction both` or `dot1x control-direction both` interface configuration command, the port is access-controlled in both directions. The port does not receive packets from or send packets to the host.

802.1x Authentication with MAC Authentication Bypass

You can configure the switch to authorize clients based on the client MAC address (see Figure 10-2 on page 10-4) by using the MAC authentication bypass feature. For example, you can enable this feature on 802.1x ports connected to devices such as printers.

If 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 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 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.

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 802.1x supplicant, the switch does not unauthorize the client connected to the port. When re-authentication occurs, the switch uses 802.1x authentication as the preferred re-authentication process 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 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 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, “802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.”

MAC authentication bypass interacts with the features:

- 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 802.1x port is authenticated with MAC authentication bypass.

• Port security—See the “802.1x Authentication with Port Security” section on page 10-25.

• Voice VLAN—See the “802.1x Authentication with Voice VLAN Ports” section on page 10-25.

• VLAN Membership Policy Server (VMPS)—802.1x and VMPS are mutually exclusive.

• Private VLAN—You can assign a client to a private VLAN.

• Network admission control (NAC) Layer 2 IP validation—This feature takes effect after an 802.1x port is authenticated with MAC authentication bypass, including hosts in the exception list.

For more configuration information, see the “Authentication Manager” section on page 10-7.

Cisco IOS Release 12.2(55)SE and later supports filtering of verbose MAB system messages. See the “Authentication Manager CLI Commands” section on page 10-9.

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.

For more information, see the “Configuring 802.1x User Distribution” section on page 10-60.

**Network Admission Control Layer 2 802.1x Validation**

The switch supports the Network Admission Control (NAC) Layer 2 802.1x validation, which checks the antivirus condition or posture of endpoint systems or clients before granting the devices network access. With NAC Layer 2 802.1x validation, you can do these tasks:

• Download the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]) from the authentication server.

• Set the number of seconds between re-authentication attempts as the value of the Session-Timeout RADIUS attribute (Attribute[27]) and get an access policy against the client from the RADIUS server.

• Set the action to be taken when the switch tries to re-authenticate the client by using the Termination-Action RADIUS attribute (Attribute[29]). If the value is the DEFAULT or is not set, the session ends. If the value is RADIUS-Request, the re-authentication process starts.

• Set the list of VLAN number or name or VLAN group name as the value of the Tunnel Group Private ID (Attribute[81]) and the preference for the VLAN number or name or VLAN group name as the value of the Tunnel Preference (Attribute[83]). If you do not configure the Tunnel Preference, the first Tunnel Group Private ID (Attribute[81]) attribute is picked up from the list.

• View the NAC posture token, which shows the posture of the client, by using the `show authentication` or `show dot1x` privileged EXEC command.

• Configure secondary private VLANs as guest VLANs.

Configuring NAC Layer 2 802.1x validation is similar to configuring 802.1x port-based authentication except that you must configure a posture token on the RADIUS server. For information about configuring NAC Layer 2 802.1x validation, see the “Configuring NAC Layer 2 802.1x Validation” section on page 10-61 and the “Configuring Periodic Re-Authentication” section on page 10-45.

For more information about NAC, see the *Network Admission Control Software Configuration Guide*.

For more configuration information, see the “Authentication Manager” section on page 10-7.

**Flexible Authentication Ordering**

You can use flexible authentication ordering to configure the order of methods that a port uses to authenticate a new host. 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. For more information see the “Configuring Flexible Authentication Ordering” section on page 10-67.
Open1x Authentication

Open1x authentication allows a device access to a port before that device is authenticated. When open authentication is configured, a new host on the port can only send traffic to the switch. 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.

For more information see the “Configuring the Host Mode” section on page 10-44.

Using Voice Aware 802.1x Security

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. When an attempt to authenticate the data client caused a security violation in previous releases, the entire port shut down, resulting in a complete loss of connectivity.

You can use this feature where a PC is connected to the IP phone. A security violation found on the data VLAN shuts down only the data VLAN. The traffic on the voice VLAN continues without interruption.

For information on configuring voice aware 802.1x security, see the “Configuring Voice Aware 802.1x Security” section on page 10-38.

802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)

The Network Edge Access Topology (NEAT) feature extends identity to areas outside the wiring closet (such as conference rooms). This allows any type of device to authenticate on the port.

- 802.1x switch supplicant: You can configure a switch to act as a supplicant to another switch by using the 802.1x supplicant feature. This configuration is helpful in a scenario, where, for example, a switch is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1x switch supplicant feature authenticates with the upstream switch for secure connectivity.

  Once the supplicant switch authenticates successfully the port mode changes from access to trunk.

- If the access VLAN is configured on the authenticator switch, it becomes the native VLAN for the trunk port after successful authentication.

You can enable MDA or multiauth mode on the authenticator switch interface that connects to one more supplicant switches. Multihost mode is not supported on the authenticator switch interface.
Use the `dot1x supplicant force-multicast` global configuration command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

- **Host Authorization:** Ensures that only traffic from authorized hosts (connecting to the switch with supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting to the supplicant switch to the authenticator switch, as shown in Figure 10-6.

- **Auto enablement:** Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs coming from supplicant switches. Configure the `cisco-av-pair` as `device-traffic-class=switch` at the ACS. (You can configure this under the group or the user settings.)

### Figure 10-6 Authenticator and Supplicant Switch using CISP

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Workstations (clients)</td>
</tr>
<tr>
<td>3</td>
<td>Authenticator switch</td>
</tr>
<tr>
<td>5</td>
<td>Trunk port</td>
</tr>
<tr>
<td>2</td>
<td>Supplicant switch (outside wiring closet)</td>
</tr>
<tr>
<td>4</td>
<td>Access control server (ACS)</td>
</tr>
</tbody>
</table>

### Guidelines

- You can configure NEAT ports with the same configurations as the other authentication ports. When the supplicant switch authenticates, the port mode is changed from `access` to `trunk` based on the switch vendor-specific attributes (VSAs). (device-traffic-class=switch).

- The VSA changes the authenticator switch port mode from access to trunk and enables 802.1x trunk encapsulation and the access VLAN if any would be converted to a native trunk VLAN. VSA does not change any of the port configurations on the supplicant.

- To change the host mode and the apply a standard port configuration on the authenticator switch port, you can also use Auto Smartports user-defined macros, instead of the switch VSA. This allows you to remove unsupported configurations on the authenticator switch port and to change the port mode from `access` to `trunk`. For information, see the *AutoSmartports Configuration Guide.*

For more information, see the “Configuring an Authenticator and a Supplicant Switch with NEAT” section on page 10-62.
Chapter 10  Configuring IEEE 802.1x Port-Based Authentication

Using IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute

The switch supports both IP standard and IP extended port access control lists (ACLs) applied to ingress ports.

- ACLs that you configure
- ACLs from the Access Control Server (ACS)

An IEEE 802.1x port in single-host mode uses ACLs from the ACS to provide different levels of service to an IEEE 802.1x-authenticated user. When the RADIUS server authenticates this type of user and port, it sends ACL attributes based on the user identity to the switch. The switch applies the attributes to the port for the duration of the user session. If the session is over, authentication fails, or a link fails, the port becomes unauthorized, and the switch removes the ACL from the port.

Only IP standard and IP extended port ACLs from the ACS support the Filter-Id attribute. It specifies the name or number of an ACL. The Filter-id attribute can also specify the direction (inbound or outbound) and a user or a group to which the user belongs.

- The Filter-Id attribute for the user takes precedence over that for the group.
- If a Filter-Id attribute from the ACS specifies an ACL that is already configured, it takes precedence over a user-configured ACL.
- If the RADIUS server sends more than one Filter-Id attribute, only the last attribute is applied.

If the Filter-Id attribute is not defined on the switch, authentication fails, and the port returns to the unauthorized state.

Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the show authentication command. The session ID in this example is 16000005000000B288508E5:

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  16000005000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also16000005000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000005000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000005000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000005000000B288508E5
```
The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

### Configuring 802.1x Authentication

These sections contain this configuration information:

- Default 802.1x Authentication Configuration, page 10-34
- 802.1x Authentication Configuration Guidelines, page 10-35
- Configuring 802.1x Readiness Check, page 10-37 (optional)
- Configuring Voice Aware 802.1x Security, page 10-38 (optional)
- Configuring 802.1x Violation Modes, page 10-40 (optional)
- Configuring the Switch-to-RADIUS-Server Communication, page 10-43 (required)
- Configuring the Host Mode, page 10-44 (optional)
- Configuring Periodic Re-Authentication, page 10-45 (optional)
- Manually Re-Authenticating a Client Connected to a Port, page 10-47 (optional)
- Changing the Quiet Period, page 10-47 (optional)
- Changing the Switch-to-Client Retransmission Time, page 10-48 (optional)
- Setting the Switch-to-Client Frame-Retransmission Number, page 10-49 (optional)
- Setting the Re-Authentication Number, page 10-50 (optional)
- Configuring 802.1x Accounting, page 10-52 (optional)
- Enabling MAC Move, page 10-51 (optional)
- Enabling MAC Replace, page 10-51 (optional)
- Configuring a Guest VLAN, page 10-53 (optional)
- Configuring a Restricted VLAN, page 10-54 (optional)
- Configuring Inaccessible Authentication Bypass and Critical Voice VLAN, page 10-56 (optional)
- Configuring 802.1x Authentication with WoL, page 10-58 (optional)
- Configuring MAC Authentication Bypass, page 10-59 (optional)
- Configuring NAC Layer 2 802.1x Validation, page 10-61 (optional)
- Configuring an Authenticator and a Supplicant Switch with NEAT, page 10-62
- Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs, page 10-63
- Configuring Flexible Authentication Ordering, page 10-67
- Disabling 802.1x Authentication on the Port, page 10-68 (optional)
- Resetting the 802.1x Authentication Configuration to the Default Values, page 10-69 (optional)
Default 802.1x Authentication Configuration

Table 10-4 shows the default 802.1x authentication configuration.

**Table 10-4 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></td>
</tr>
<tr>
<td>- IP address</td>
<td>None specified.</td>
</tr>
<tr>
<td>- UDP authentication port</td>
<td>1812.</td>
</tr>
<tr>
<td>- Key</td>
<td>None specified.</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.)</td>
</tr>
<tr>
<td>You can change this timeout period by using the authentication timer server or dot1x timeout server-timeout interface configuration command.</td>
<td></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>
</tbody>
</table>
Chapter 10 Configuring IEEE 802.1x Port-Based Authentication

Configuring 802.1x Authentication

802.1x Authentication Configuration Guidelines

These section has configuration guidelines for these features:

- 802.1x Authentication, page 10-35
- VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass, page 10-36
- MAC Authentication Bypass, page 10-37
- Maximum Number of Allowed Devices Per Port, page 10-37

802.1x Authentication

- When 802.1x authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- If you try to change the mode of an 802.1x-enabled port (for example, from access to trunk), an error message appears, and the port mode is not changed.
- 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:
  - Trunk port—If you try to enable 802.1x authentication on a trunk 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 trunk, an error message appears, and the port mode is not changed.
  - 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.
  - Dynamic-access ports—If you try to enable 802.1x authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1x authentication is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC authentication bypass</td>
<td>Disabled</td>
</tr>
<tr>
<td>Voice-aware security</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Table 10-4 Default 802.1x Authentication Configuration (continued)
Chapter 10 Configuring IEEE 802.1x Port-Based Authentication

Configuring 802.1x Authentication

- 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. See the “Authentication Manager CLI Commands” section on page 10-9.

VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass

- When 802.1x authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- The 802.1x authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.
- You can configure 802.1x authentication on a private-VLAN port, but do not configure 802.1x authentication with port security, a voice VLAN, a guest VLAN, a restricted VLAN, or a per-user ACL on private-VLAN ports.
- You can configure any VLAN except an RSPAN VLAN, private VLAN, or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- After you configure a guest VLAN for an 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the 802.1x authentication process (authentication timer inactivity or dot1x timeout quiet-period) and authentication timer reauthentication or dot1x timeout tx-period) interface configuration commands). The amount to decrease the settings depends on the connected 802.1x client type.

- When configuring the inaccessible authentication bypass feature, follow these guidelines:
  - The feature is supported on 802.1x port in single-host mode and multihosts mode.
  - If the client is running Windows XP and the port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.
  - If the Windows XP client is configured for DHCP and has an IP address from the DHCP server, receiving an EAP-Success message on a critical port might not re-initiate the DHCP configuration process.
  - You can configure the inaccessible authentication bypass feature and the restricted VLAN on an 802.1x port. If the switch tries to re-authenticate a critical port in a restricted VLAN and all the RADIUS servers are unavailable, switch changes the port state to the critical authentication state and remains in the restricted VLAN.
  - You can configure the inaccessible bypass feature and port security on the same switch port.
  - You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
MAC Authentication Bypass

- Unless otherwise stated, the MAC authentication bypass guidelines are the same as the 802.1x authentication guidelines. For more information, see the “802.1x Authentication” section on page 10-35.
- 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. You must enable port security before configuring a timeout value. For more information, see the “Configuring Port Security” section on page 25-9.

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 multiple-host mode, only one 802.1x supplicant is allowed on the port, but an unlimited number of non-802.1x hosts are allowed on the access VLAN. An unlimited number of devices are allowed on the voice VLAN.

Configuring 802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable.

The 802.1x readiness check is allowed on all ports that can be configured for 802.1x. The readiness check is not available on a port that is configured as `dot1x force-unauthorized`.

Follow these guidelines to enable the readiness check on the switch:

- The readiness check is typically used before 802.1x is enabled on the switch.
- If you use the `dot1x test eapol-capable` privileged EXEC command without specifying an interface, all the ports on the switch stack are tested.
- When you configure the `dot1x test eapol-capable` command on an 802.1x-enabled port, and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is 802.1x-capable. A syslog message is generated if the client responds within the timeout period. If the client does not respond to the query, the client is not 802.1x-capable. No syslog message is generated.
- The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). A syslog message is generated for each of the clients that respond to the readiness check within the timer period.
Beginning in privileged EXEC mode, follow these steps to enable the 802.1x readiness check on the switch:

### Command | Purpose
--- | ---
**Step 1** | 
1. `dot1x test eapol-capable [interface interface-id]`  
   Enable the 802.1x readiness check on the switch.  
   (Optional) For `interface-id` specify the port on which to check for 802.1x readiness.  
   **Note** If you omit the optional `interface` keyword, all interfaces on the switch are tested.  
2. `configure terminal`  
   (Optional) Enter global configuration mode.  
3. `dot1x test timeout timeout`  
   (Optional) Configure the timeout used to wait for EAPOL response. The range is from 1 to 65535 seconds. The default is 10 seconds.  
4. `end`  
   (Optional) Return to privileged EXEC mode.  
5. `show running-config`  
   (Optional) Verify your modified timeout values.

This example shows how to enable a readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is 802.1x-capable:

---

### Configuring Voice Aware 802.1x Security

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>errdisable detect cause security-violation shutdown vlan</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the <strong>shutdown vlan</strong> keywords are not included, the entire port enters the error-disabled state and shuts down.</td>
</tr>
<tr>
<td>Step 3</td>
<td>errdisable recovery cause security-violation</td>
</tr>
<tr>
<td>Step 4</td>
<td>clear errdisable interface interface-id vlan [vlan-list]</td>
</tr>
<tr>
<td></td>
<td>• For <strong>interface-id</strong> specify the port on which to reenable individual VLANs.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <strong>vlan-list</strong> specify a list of VLANs to be re-enabled. If <strong>vlan-list</strong> is not specified, all VLANs are re-enabled.</td>
</tr>
<tr>
<td>Step 5</td>
<td>shutdown no-shutdown</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show errdisable detect</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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 0/2.

```
Switch# clear errdisable interface gigabitethernet0/2 vlan
```

You can verify your settings by entering the **show errdisable detect** privileged EXEC command.
### 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa authentication dot1x {default} method1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switchport mode access</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>authentication violation shutdown</td>
</tr>
<tr>
<td></td>
<td>restrict</td>
</tr>
<tr>
<td></td>
<td>protect</td>
</tr>
<tr>
<td></td>
<td>replace</td>
</tr>
<tr>
<td></td>
<td>dot1x violation-mode {shutdown</td>
</tr>
<tr>
<td></td>
<td>restrict</td>
</tr>
<tr>
<td></td>
<td>protect</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show authentication</td>
</tr>
<tr>
<td>or</td>
<td>show dot1x</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
Configuring 802.1x Authentication

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.

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:

**Step 1** A user connects to a port on the switch.

**Step 2** Authentication is performed.

**Step 3** VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.

**Step 4** The switch sends a start message to an accounting server.

**Step 5** Re-authentication is performed, as necessary.

**Step 6** The switch sends an interim accounting update to the accounting server, that is based on the result of re-authentication.

**Step 7** The user disconnects from the port.

**Step 8** The switch sends a stop message to the accounting server.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td></td>
<td>Enable AAA.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa authentication dot1x {default} method1</td>
</tr>
<tr>
<td></td>
<td>Create an 802.1x authentication method list.</td>
</tr>
<tr>
<td></td>
<td>To create a default list to use when a named list is <em>not</em> specified in the authentication command, use the default keyword followed by the method to use in default situations. The default method list is automatically applied to all ports.</td>
</tr>
<tr>
<td></td>
<td>For method1, enter the group radius keywords to use the list of all RADIUS servers for authentication.</td>
</tr>
<tr>
<td></td>
<td>Note Though other keywords are visible in the command-line help string, only the group radius keywords are supported.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>dot1x system-auth-control</td>
</tr>
<tr>
<td></td>
<td>Enable 802.1x authentication globally on the switch.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>aaa authorization network {default} group radius</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure 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></td>
<td>For per-user ACLs, single-host mode must be configured. This setting is the default.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>radius-server host ip-address</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>radius-server key string</td>
</tr>
<tr>
<td></td>
<td>(Optional) Specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
</tbody>
</table>
### Configuring 802.1x Port-Based Authentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>switchport mode access</code></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>authentication port-control auto</code> or <code>dot1x port-control auto</code></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>show authentication</code> or <code>show dot1x</code></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
Chapter 10 Configuring IEEE 802.1x Port-Based Authentication

Configuring 802.1x Authentication

Configuring the 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 the 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 in which they were configured.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>radius-server host {hostname</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To clear the specified RADIUS server, use the **no radius-server host {hostname | ip-address}** global configuration command.

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to **rad123**, matching the key on the RADIUS server:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

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**, **radius-server retransmit** and the **radius-server key** global configuration commands. For more information, see the “Configuring Settings for All RADIUS Servers” section on page 8-35.
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.

## Configuring the Host Mode

Beginning in privileged EXEC mode, follow these steps to allow a single host (client) or multiple hosts on an 802.1x-authorized port. Use the **multi-domain** keyword to configure multidomain authentication (MDA) to enable authentication of 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</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>radius-server vsa send authentication</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>authentication host-mode [multi-auth</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>dot1x host-mode [single-host</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>switchport voice vlan vlan-id</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
</tbody>
</table>

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure the network access server to recognize and use vendor-specific attributes (VSAs).</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specify the port to which multiple hosts are indirectly attached, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>multi-auth</strong>—Allow one client on the voice VLAN and multiple authenticated clients on the data VLAN. Each host is individually authenticated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>multi-host</strong>—Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>multi-domain</strong>—Allow both a host and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an 802.1x-authorized port.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Configure the voice VLAN.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Notes

- You must configure the voice VLAN for the IP phone when the host mode is set to **multi-domain**. For more information, see Chapter 15, “Configuring Voice VLAN.”

- Make sure that the authentication port-control or dot1x port-control interface configuration command set is set to **auto** for the specified interface.
Configuring IEEE 802.1x Port-Based Authentication

Configuring 802.1x Authentication

To disable multiple hosts on the port, use the **no authentication host-mode** or the **no dot1x host-mode multi-host** interface configuration command.

This example shows how to enable 802.1x authentication and to allow multiple hosts:

```
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

This example shows how to enable MDA and to allow both a host and a voice device on the port:

```
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# switchport voice vlan 101
Switch(config-if)# end
```

**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.

<table>
<thead>
<tr>
<th>Command</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>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>authentication periodic</code></td>
<td>Enable periodic re-authentication of the client, which is disabled by</td>
</tr>
<tr>
<td>or</td>
<td>default.</td>
</tr>
<tr>
<td><code>dot1x reauthentication</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring 802.1x Port-Based Authentication

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication timer</code> `{ {inactivity</td>
<td>reauthenticate} } { restart value }`</td>
</tr>
<tr>
<td>or <code>dot1x timeout reauth-period</code> `{ seconds</td>
<td>server }`</td>
</tr>
<tr>
<td></td>
<td>• <code>reauthenticate</code>—Time in seconds after which an automatic re-authentication attempt is be initiated</td>
</tr>
<tr>
<td></td>
<td>• <code>restart value</code>—Interval in seconds after which an attempt is made to authenticate an unauthorized port</td>
</tr>
</tbody>
</table>

The `dot1x timeout reauth-period` keywords have these meanings:

- `seconds`—Sets the number of seconds from 1 to 65535; the default is 3600 seconds.
- `server`—Sets the number of seconds based on the value of the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

This command affects the behavior of the switch only if periodic re-authentication is enabled.

**Step 5**

`end`

Return to privileged EXEC mode.

**Step 6**

- `show authentication interface-id`
- `show dot1x interface interface-id`

Verify your entries.

**Step 7**

`copy running-config startup-config`

(Optional) Save your entries in the configuration file.

---

To disable periodic re-authentication, use the `no authentication periodic` or the `no dot1x reauthentication` interface configuration command. To return to the default number of seconds between re-authentication attempts, use the `no authentication timer` or the `no dot1x timeout reauth-period` interface configuration command.

This example shows how to enable periodic re-authentication and set the number of seconds between re-authentication attempts to 4000:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```
Manually Re-Authenticating a Client Connected to a Port

You can manually re-authenticate the client connected to a specific port at any time by entering the `dot1x re-authenticate interface interface-id` privileged EXEC command. This step is optional. If you want to enable or disable periodic re-authentication, see the “Configuring Periodic Re-Authentication” section on page 10-45.

This example shows how to manually re-authenticate the client connected to a port:

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 `dot1x timeout quiet-period` interface configuration command controls the idle period. A failed client authentication 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>dot1x timeout quiet-period seconds</td>
<td>Set the number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show authentication interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>or show dot1x interface interface-id</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default quiet time, use the `no dot1x timeout quiet-period` interface configuration command.

This example shows how to set the quiet time on the switch to 30 seconds:

```
Switch(config-if)# dot1x timeout quiet-period 30
```
### Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then resends the frame.

**Note**
You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to change the amount of time that the switch waits for client notification. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to configure, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 dot1x timeout tx-period seconds</td>
<td>Set the number of seconds that the switch waits for a response to an</td>
</tr>
<tr>
<td></td>
<td>EAP-request/identity frame from the client before resending the request.</td>
</tr>
<tr>
<td></td>
<td>The range is 1 to 65535 seconds; the default is 5.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show authentication interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default retransmission time, use the `no dot1x timeout tx-period` interface configuration command.

This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request:

```
Switch(config-if)# dot1x timeout tx-period 60
```
Setting the Switch-to-Client Frame-Retransmission Number

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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1:  configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2:  interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3:  dot1x max-reauth-req count</td>
<td>Set 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>Step 4:  end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5:  show authentication interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>or show dot1x interface interface-id</td>
<td></td>
</tr>
<tr>
<td>Step 6:  copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default retransmission number, use the **no dot1x max-req** interface configuration command.

This example shows how to set 5 as the number of times that the switch sends an EAP-request/identity request before restarting the authentication process:

```
Switch(config-if)# dot1x max-req 5
```
### 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.

**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 re-authentication number. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>dot1x max-reauth-req count</td>
<td>Set 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>Step 4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show authentication interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show dot1x interface interface-id</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default re-authentication number, use the `no dot1x max-reauth-req` interface configuration command.

This example shows how to set 4 as the number of times that the switch restarts the authentication process before the port changes to the unauthorized state:

```
Switch(config-if)# dot1x max-reauth-req 4
```
## 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>authentication mac-move permit</strong></td>
</tr>
<tr>
<td></td>
<td>Enable MAC move on the switch.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>show running-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to globally enable MAC move on a switch:

```
Switch(config)# authentication mac-move permit
```

## 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**authentication violation { protect</td>
</tr>
<tr>
<td></td>
<td>Use the replace keyword to enable MAC replace on the interface. The port removes the current session and initiates authentication with the new host. The other keywords have these effects:</td>
</tr>
<tr>
<td></td>
<td>• <strong>protect</strong>: the port drops packets with unexpected MAC addresses without generating a system message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>restrict</strong>: violating packets are dropped by the CPU and a system message is generated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>shutdown</strong>: the port is error disabled when it receives an unexpected MAC address.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEc mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>show running-config</strong></td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable MAC replace on an interface:

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# authentication violation replace
```
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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>aaa accounting dot1x default start-stop group radius</td>
<td>Enable 802.1x accounting using the list of all RADIUS servers.</td>
</tr>
<tr>
<td>4</td>
<td>aaa accounting system default start-stop group radius</td>
<td>(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEc mode.</td>
</tr>
<tr>
<td>6</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the show radius statistics privileged EXEC command to display the number of RADIUS messages that do not receive the accounting response message.

This example shows how to configure 802.1x accounting. The first command configures the RADIUS server, specifying 1813 as the UDP port for accounting:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
```
**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.

To disable and remove the guest VLAN, use the `no dot1x guest-vlan` interface configuration command. The port returns to the unauthorized state.

This example shows how to enable VLAN 2 as an 802.1x guest VLAN:

```
Switch(config-if)# dot1x guest-vlan 2
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before re-sending the request, and to enable VLAN 2 as an 802.1x guest VLAN when an 802.1x port is connected to a DHCP client:

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the “802.1x Authentication Configuration Guidelines” section on page 10-35.</td>
</tr>
<tr>
<td></td>
<td>switchport mode access</td>
<td>Set the port to access mode.</td>
</tr>
<tr>
<td></td>
<td>switchport mode private-vlan host</td>
<td>Configure the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td></td>
<td>authentication port-control auto</td>
<td>Enable 802.1x authentication on the port.</td>
</tr>
<tr>
<td></td>
<td>dot1x port-control auto</td>
<td>Specify 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, a primary private VLAN, or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>show authentication interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>show dot1x interface interface-id</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable and remove the guest VLAN, use the `no dot1x guest-vlan` interface configuration command. The port returns to the unauthorized state.
Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch, clients that are 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.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure terminal</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the “802.1x Authentication Configuration Guidelines” section on page 10-35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode access or switchport mode private-vlan host</td>
<td>Set the port to access mode, or Configure the Layer 2 port as a private-VLAN host port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>authentication port-control auto or dot1x port-control auto</td>
<td>Enable 80.1x authentication on the port.</td>
</tr>
<tr>
<td>Step 5</td>
<td>authentication event fail action authorize vlan-id</td>
<td>Specify 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, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN.</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>show authentication interface-id or show dot1x interface interface-id</td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable and remove the restricted VLAN, use the no dot1x auth-fail vlan interface configuration command. The port returns to the unauthorized state.

This example shows how to enable VLAN 2 as an 802.1x restricted VLAN:

```
Switch(config-if)# dot1x auth-fail vlan 2
```

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the dot1x auth-fail max-attempts 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the “802.1x Authentication Configuration Guidelines” section on page 10-35.</td>
</tr>
<tr>
<td>Step 3 switchport mode access</td>
<td>Set the port to access mode, or switchport mode private-vlan host</td>
</tr>
<tr>
<td>Step 4 authentication port-control auto</td>
<td>Enable 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Step 5 dot1x auth-fail vlan vlan-id</td>
<td>Specify 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, a primary private VLAN, or a voice VLAN as an 802.1x restricted VLAN.</td>
</tr>
<tr>
<td>Step 6 dot1x auth-fail max-attempts max attempts</td>
<td>Specify a number of authentication attempts to allow before a port moves to the restricted VLAN. The range is 1 to 3, and the default is 3.</td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 8 show authentication interface-id</td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td>Step 9 show dot1x interface interface-id</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>Step 10 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default value, use the no dot1x auth-fail max-attempts interface configuration command.

This example shows how to set 2 as the number of authentication attempts allowed before the port moves to the restricted VLAN:

```
Switch(config-if)# dot1x auth-fail max-attempts 2
```
Chapter 10  Configuring IEEE 802.1x Port-Based Authentication

Configuring Inaccessible Authentication Bypass and Critical Voice VLAN

You can configure the inaccessible bypass feature, also referred to as critical authentication or the AAA fail policy to allow data traffic to pass through on the native VLAN when the server is not available. You can also configure the critical voice VLAN feature so that if the server is not available and traffic from the host is tagged with the voice VLAN, the connected device (the phone) is put in the configured voice VLAN for the port.

Beginning in privileged EXEC mode, follow these steps to configure critical voice VLAN on a port and enable the inaccessible authentication bypass feature.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>radius-server dead-criteria time (t) tries (t)</td>
<td>Sets the conditions that are used to decide when a RADIUS server is considered unavailable or down (dead).</td>
</tr>
<tr>
<td>(t)</td>
<td>The range for (t) is from 1 to 120 seconds. The switch dynamically determines a default (t) value between 10 and 60 seconds.</td>
</tr>
<tr>
<td>(t)</td>
<td>The range for (t) is from 1 to 100. The switch dynamically determines a default (t) parameter between 10 and 100.</td>
</tr>
<tr>
<td>radius-server deadtime minutes</td>
<td>(Optional) Sets the number of minutes during which a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.</td>
</tr>
<tr>
<td>radius-server host ip-address [acct-port udp-port] [auth-port udp-port] [test username name] [idle-time time] [ignore-acct-port] [ignore-auth-port] [key string]</td>
<td>Configures the RADIUS server parameters:</td>
</tr>
<tr>
<td>(acct-port) udp-port</td>
<td>Specifies the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646.</td>
</tr>
<tr>
<td>(auth-port) udp-port</td>
<td>Specifies the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645.</td>
</tr>
<tr>
<td>Note</td>
<td>You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values.</td>
</tr>
<tr>
<td>test username name</td>
<td>Enables automatic testing of the RADIUS server status, and specifies the username to be used.</td>
</tr>
<tr>
<td>idle-time time</td>
<td>Sets 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).</td>
</tr>
<tr>
<td>ignore-acct-port</td>
<td>Disables testing on the RADIUS-server accounting port.</td>
</tr>
<tr>
<td>ignore-auth-port</td>
<td>Disables testing on the RADIUS-server authentication port.</td>
</tr>
<tr>
<td>key string</td>
<td>For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
</tr>
</tbody>
</table>

You can also configure the authentication and encryption key by using the radius-server key \(0\ string \mid 7\ string \mid string\) global configuration command.
Chapter 10  Configuring IEEE 802.1x Port-Based Authentication

Configuring 802.1x Authentication

This example shows how to configure the inaccessible authentication bypass feature and configure the critical voice VLAN:

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)# interface gigabitethernet 1/0/1
Switch(config)# radius-server deadtime 60
Switch(config-if)# authentication event server dead action reinitialize vlan 20
Switch(config-if)# switchport voice vlan
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# end

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>
| **Step 6** | authentication event server dead action {authorize | reinitialize} vlan vlan-id | Configures a critical VLAN to move hosts on the port if the RADIUS server is unreachable:  
  - **authorize**—Moves any new hosts trying to authenticate to the user-specified critical VLAN.  
  - **reinitialize**—Moves all authorized hosts on the port to the user-specified critical VLAN. |
| **Step 7** | switchport voice vlan vlan-id | Specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6. |
| **Step 8** | 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 9** | end | Returns to privileged EXEC mode. |
| **Step 10** | show authentication interface interface-id | (Optional) Verifies your entries. |
### Configuring 802.1x Authentication with WoL

Beginning in privileged EXEC mode, follow these steps to enable 802.1x authentication with WoL. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>authentication control-direction {both</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show authentication interface interface-id or show dot1x interface interface-id</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable 802.1x authentication with WoL, use the `no authentication control-direction` or `no dot1x control-direction` interface configuration command.

These examples show how to enable 802.1x authentication with WoL and set the port as bidirectional:

```
Switch(config-if)# authentication control-direction both
```

or

```
Switch(config-if)# dot1x control-direction both
```
### Configuring MAC Authentication Bypass

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication bypass. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the “802.1x Authentication Configuration Guidelines” section on page 10-35.</td>
</tr>
<tr>
<td>Step 3</td>
<td>authentication port-control auto</td>
<td>Enable 802.1x authentication on the port.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>dot1x port-control auto</td>
</tr>
<tr>
<td>Step 4</td>
<td>mab [eap</td>
<td>timeout activity {value}]</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show authentication interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td>show dot1x interface interface-id</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable MAC authentication bypass, use the **no mab** interface configuration command.

This example shows how to enable MAC authentication bypass:

```
Switch(config-if)# mab
```
Configuring 802.1x User Distribution

Beginning in global configuration, follow these steps to configure a VLAN group and to map a VLAN to it:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Vlan group</strong> vlan-group-name vlan-list vlan-list**</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>show vlan group</strong> all vlan-group-name**</td>
</tr>
<tr>
<td>Step 3</td>
<td><strong>no vlan group</strong> vlan-group-name vlan-list vlan-list**</td>
</tr>
</tbody>
</table>

This example shows how to configure the VLAN groups, to map the VLANs to the groups, to and verify the VLAN group configurations and mapping to the specified VLANs:

```
switch(config)# vlan group eng-dept vlan-list 10
switch(config)# show vlan group group-name eng-dept
Group Name    Vlans Mapped
------------- --------------
eng-dept      10
```

This example shows how to add a VLAN to an existing VLAN group and to verify that the VLAN was added:

```
switch(config)# vlan group eng-dept vlan-list 30
switch(config)# show vlan group eng-dept
Group Name    Vlans Mapped
------------- --------------
eng-dept      10,30
hr-dept       20
```

This example shows how to remove a VLAN from a VLAN group:

```
switch# no vlan group eng-dept vlan-list 10
```

This example shows how to clear all the VLANs are cleared from a VLAN group, the VLAN group is cleared:

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
switch(config)# show vlan group group-name eng-dept
```

This example shows how to clear all the VLAN groups:

```
switch(config)# no vlan group end-dept vlan-list all
switch(config)# show vlan-group all
```

For more information about these commands, see the *Cisco IOS Security Command Reference*. 
### Configuring NAC Layer 2 802.1x Validation

You can configure NAC Layer 2 802.1x validation, which is also referred to as 802.1x authentication with a RADIUS server.

Beginning in privileged EXEC mode, follow these steps to configure NAC Layer 2 802.1x validation. The procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>dot1x guest-vlan vlan-id</td>
<td>Specify an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, or a voice VLAN as an 802.1x guest VLAN.</td>
</tr>
<tr>
<td></td>
<td>authentication periodic</td>
<td>Enable periodic re-authentication of the client, which is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dot1x reauthentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dot1x timeout reauth-period {seconds</td>
<td>server}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- seconds—Sets the number of seconds from 1 to 65535. The default is 3600 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- server—Sets the number of seconds based on the value of the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]). This command affects the behavior of the switch only if periodic re-authentication is enabled.</td>
</tr>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>show authentication interface interface-id</td>
<td>Verify your 802.1x authentication configuration.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show dot1x interface interface-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure NAC Layer 2 802.1x validation:

Switch# configure terminal
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period server
## Configuring an Authenticator and a Supplicant Switch with NEAT

Configuring this feature requires that one switch outside a wiring closet is configured as a supplicant and is connected to an authenticator switch.

For overview information, see the “802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)” section on page 10-30.

### Note

The *cisco-av-pairs* must be configured as *device-traffic-class=switch* on the ACS, which sets the interface as a trunk after the supplicant is successfully authenticated.

Beginning in privileged EXEC mode, follow these steps to configure a switch as an authenticator:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><em>configure terminal</em></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><em>cisp enable</em></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><em>interface interface-id</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><em>switchport mode access</em></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><em>authentication port-control auto</em></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><em>dot1x pae authenticator</em></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><em>spanning-tree portfast</em></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><em>end</em></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><em>show running-config interface interface-id</em></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><em>copy running-config startup-config</em></td>
</tr>
</tbody>
</table>

This example shows how to configure a switch as an 802.1x authenticator:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

Beginning in privileged EXEC mode, follow these steps to configure a switch as a supplicant:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><em>configure terminal</em></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><em>cisp enable</em></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><em>dot1x credentials profile</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><em>username suppswitch</em></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><em>password password</em></td>
</tr>
</tbody>
</table>
Chapter 10  Configuring IEEE 802.1x Port-Based Authentication

Configuring 802.1x Authentication

**Step 6**
```
dot1x supplicant force-multicast
```
Force the switch to send only multicast EAPOL packets when it receives either unicast or multicast packets.

This also allows NEAT to work on the supplicant switch in all host modes.

**Step 7**
```
interface interface-id
```
Specify the port to be configured, and enter interface configuration mode.

**Step 8**
```
switchport trunk encapsulation dot1q
```
Set the port to trunk mode.

**Step 9**
```
switchport mode trunk
```
Configure the port as a VLAN trunk port.

**Step 10**
```
dot1x pae supplicant
```
Configure the interface as a port access entity (PAE) supplicant.

**Step 11**
```
dot1x credentials profile-name
```
Attach the 802.1x credentials profile to the interface.

**Step 12**
```
end
```
Return to privileged EXEC mode.

**Step 13**
```
show running-config interface interface-id
```
Verify your configuration.

**Step 14**
```
copy running-config startup-config
```
(Optional) Save your entries in the configuration file.

This example shows how to configure a switch as a supplicant:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

**Configuring NEAT with Auto Smartports Macros**

You can also use an Auto Smartports user-defined macro instead of the switch VSA to configure the authenticator switch. For information, see the Auto Smartports Configuration Guide.

**Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs**

In addition to configuring 802.1x authentication on the switch, you need to configure the ACS. For more information, see the Cisco Secure ACS configuration guides.

**Note**
You must configure a downloadable ACL on the ACS before downloading it to the switch.

After authentication on the port, you can use the `show ip access-list` privileged EXEC command to display the downloaded ACLs on the port.
Configuring Downloadable ACLs

The policies take effect after client authentication and the client IP address addition to the IP device tracking table. The switch then applies the downloadable ACL to the port.

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</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> ip device tracking</td>
<td>Configure the ip device tracking table.</td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td><strong>Step 4</strong> aaa authorization network default group</td>
<td>Sets the authorization method to local. To remove the authorization method, use the <strong>no aaa authorization network default group radius</strong> command.</td>
</tr>
<tr>
<td><strong>Step 5</strong> radius-server vsa send authentication</td>
<td>Configure the radius vsa send authentication.</td>
</tr>
<tr>
<td><strong>Step 6</strong> interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> ip access-group acl-id in</td>
<td>Configure the default ACL on the port in the input direction.</td>
</tr>
<tr>
<td><strong>Step 8</strong> show running-config interface interface-id</td>
<td>Verify your configuration.</td>
</tr>
<tr>
<td><strong>Step 9</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**Note**: The acl-id is an access list name or number.
## Configuring a Downloadable Policy

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
</tbody>
</table>
| access-list access-list-number deny source source-wildcard log | Defines the default port ACL by using a source address and wildcard. 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. The source is the source address of the network or host that sends a packet, such as this:  
- The 32-bit quantity in dotted-decimal format.  
- The keyword any as an abbreviation for source and source-wildcard value of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard value.  
- The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0. (Optional) Applies the source-wildcard wildcard bits to the source. (Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console. |
| **Step 3**                                   |                                                                         |
| interface interface-id                       | Enter interface configuration mode.                                      |
| **Step 4**                                   |                                                                         |
| ip access-group acl-id in                    | Configure the default ACL on the port in the input direction.           |
| **Note**                                     | The acl-id is an access list name or number.                            |
| **Step 5**                                   |                                                                         |
| exit                                         | Returns to global configuration mode.                                   |
| **Step 6**                                   |                                                                         |
| aaa new-model                                | Enables AAA.                                                            |
| **Step 7**                                   |                                                                         |
| aaa authorization network default group radius | Sets the authorization method to local. To remove the authorization method, use the no aaa authorization network default group radius command.                                          |
| **Step 8**                                   |                                                                         |
| ip device tracking                           | Enables the IP device tracking table.                                   |
| To disable the IP device tracking table, use the no ip device tracking global configuration commands. |
| **Step 9**                                   |                                                                         |
| ip device tracking probe [count | interval | use-svi] | (Optional) Configures the IP device tracking table:  
- count count—Sets the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3.  
- interval interval—Sets the number of seconds that the switch waits for a response before resending the ARP probe. The range is from 30 to 300 seconds. The default is 30 seconds.  
- use-svi—Uses the switch virtual interface (SVI) IP address as source of ARP probes. |
Chapter 10  Configuring IEEE 802.1x Port-Based Authentication

Configuring 802.1x Authentication

This example shows how to configure a switch for a downloadable policy:

Switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default 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-if)# ip access-group default_acl in
Switch(config-if)# exit

Configuring VLAN ID-based MAC Authentication

Beginning in privileged EXEC mode, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 10 radius-server vsa send authentication | Configures the network access server to recognize and use vendor-specific attributes.  
**Note** The downloadable ACL must be operational. |
| Step 11 end | Returns to privileged EXEC mode. |
| Step 12 show ip device tracking all | Displays information about the entries in the IP device tracking table. |
| Step 13 copy running-config startup-config | (Optional) Saves your entries in the configuration file. |

This example shows how to globally enable VLAN ID-based MAC authentication on a switch:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mab request format attribute 32 vlan access-vlan
Switch(config-if)# exit
## Configuring Flexible Authentication Ordering

Beginning in privileged EXEC mode, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>authentication order [dot1x</td>
<td>mab]</td>
</tr>
<tr>
<td></td>
<td>{ webauth}</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>authentication priority [dot1x</td>
<td>mab]</td>
</tr>
<tr>
<td></td>
<td>{ webauth}</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>show authentication</td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure a port attempt 802.1x authentication first, followed by web authentication as fallback method:

```
Switch# configure terminal
Switch(config)# authentication order dot1x weauth
```

## Configuring Open1x

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>authentication control-direction {both</td>
<td>in}</td>
</tr>
<tr>
<td>4</td>
<td>authentication fallback name</td>
<td>(Optional) Configure a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.</td>
</tr>
<tr>
<td>5</td>
<td>authentication host-mode [multi-auth</td>
<td>multi-domain</td>
</tr>
<tr>
<td>6</td>
<td>authentication open</td>
<td>(Optional) Enable or disable open access on a port.</td>
</tr>
<tr>
<td>7</td>
<td>authentication order [dot1x</td>
<td>mab]</td>
</tr>
<tr>
<td></td>
<td>{ webauth}</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>authentication periodic</td>
<td>(Optional) Enable or disable reauthentication on a port.</td>
</tr>
<tr>
<td>9</td>
<td>authentication port-control {auto</td>
<td>force-authorized</td>
</tr>
<tr>
<td>10</td>
<td>show authentication</td>
<td>(Optional) Verify your entries.</td>
</tr>
<tr>
<td>11</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
This example shows how to configure open 802.1x on a port:

```
Switch# configure terminal
Switch(config)# authentication control-direction both
Switch(config)# authentication fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

### 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 no dot1x pae</td>
<td>Disable 802.1x authentication on the port.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show authentication</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>or show dot1x interface interface-id</td>
<td></td>
</tr>
</tbody>
</table>

To configure the port as an 802.1x port access entity (PAE) authenticator, which enables 802.1x on the port but does not allow clients connected to the port to be authorized, use the `dot1x pae authenticator` interface configuration command.

This example shows how to disable 802.1x authentication on the port:

```
Switch(config-if)# no dot1x pae authenticator
```
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and specify the port to be configured.</td>
</tr>
<tr>
<td>Step 3 dot1x default</td>
<td>Reset the 802.1x parameters to the default values.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show authentication interface</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>interface-id</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>show dot1x interface interface-id</td>
<td></td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Displaying 802.1x Statistics and Status

To display 802.1x statistics for all ports, use the show dot1x all statistics privileged EXEC command. To display 802.1x statistics for a specific port, use the show dot1x statistics interface interface-id privileged EXEC command.

To display the 802.1x administrative and operational status for the switch, use the show dot1x all [details | statistics | summary] privileged EXEC command. To display the 802.1x administrative and operational status for a specific port, use the show dot1x interface interface-id privileged EXEC command.

Beginning with Cisco IOS Release 12.2(55)SE, you can use the no dot1x logging verbose global configuration command to filter verbose 802.1x authentication messages. See the “Authentication Manager CLI Commands” section on page 10-9.

For detailed information about the fields in these displays, see the command reference for this release.
Configuring Web-Based Authentication

This chapter describes how to configure web-based authentication. It contains these sections:

- Understanding Web-Based Authentication, page 10-1
- Configuring Web-Based Authentication, page 10-9
- Displaying Web-Based Authentication Status, page 10-17

Note
For complete syntax and usage information for the switch commands used in this chapter, refer to the command reference for this release.

Understanding Web-Based Authentication

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.

Note
You can configure web-based authentication on Layer 2 and Layer 3 interfaces.

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.

These sections describe the role of web-based authentication as part of AAA:

- Device Roles, page 10-2
- Host Detection, page 10-2
- Session Creation, page 10-3
- Authentication Process, page 10-3
• Web Authentication Customizable Web Pages, page 10-6
• Web-based Authentication Interactions with Other Features, page 10-7

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 Java Script 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 10-1 shows the roles of these devices in a network:

![Figure 10-1  Web-Based Authentication Device Roles](image)

Host Detection

The switch maintains an IP device tracking table to store information about detected hosts.

**Note** 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.

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, the switch applies the failure access policy to the host. The login success page is sent to the user. (See the “Local Web Authentication Banner” section on page 10-4.)

- The switch reauthenticates a client when the host does not respond to an ARP probe on a Layer 2 interface, or when the host does not send any traffic within the idle timeout on a Layer 3 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.
Local Web Authentication Banner

You can create a banner that will appear when you log in to a switch by using web authentication. The banner appears on both the login page and the authentication-result pop-up pages.

- **Authentication Successful**
- **Authentication Failed**
- **Authentication Expired**

You create a banner by using the `ip admission auth-proxy-banner http` 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, as shown in **Figure 10-2**.

**Figure 10-2  Authentication Successful Banner**

![Authentication Successful Banner]

You can also customize the banner, as shown in **Figure 10-3**.

- Add a switch, router, or company name to the banner by using the `ip admission auth-proxy-banner http banner-text` global configuration command.
- Add a logo or text file to the banner by using the `ip admission auth-proxy-banner http file-path` 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, as shown in Figure 10-4.

For more information, see the Cisco IOS Security Command Reference and the “Configuring a Web Authentication Local Banner” section on page 10-16.
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.
- Configured pages can be accessed from the flash on the stack master or members.
- The login page can be on one flash, and the success and failure pages can be another flash (for example, the flash on the stack master or a member).
- 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, as shown in Figure 10-5 on page 10-7, 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.
For more information, see the “Customizing the Authentication Proxy Web Pages” section on page 10-13.

**Web-based Authentication Interactions with Other Features**

- Port Security, page 10-7
- LAN Port IP, page 10-8
- Gateway IP, page 10-8
- ACLs, page 10-8
- Context-Based Access Control, page 10-8
- 802.1x Authentication, page 10-8
- EtherChannel, page 10-8

**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.

For more information about enabling port security, see the “Configuring Port Security” section on page 23-9.
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.

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.

ACLs

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, you must 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.

Note: When a proxy ACL is configured for a web-based authentication client, the proxy ACL is downloaded and applied as part of the authorization process. Hence, the PACL displays the proxy ACL access control entry (ACE).

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.

802.1x Authentication

You cannot configure web-based authentication on the same port as 802.1x authentication except as a fallback authentication method.

EtherChannel

You can configure web-based authentication on a Layer 2 EtherChannel interface. The web-based authentication configuration applies to all member channels.
Configuring Web-Based Authentication

- Default Web-Based Authentication Configuration, page 10-9
- Web-Based Authentication Configuration Guidelines and Restrictions, page 10-9
- Web-Based Authentication Configuration Task List, page 10-10
- Configuring the Authentication Rule and Interfaces, page 10-10
- Configuring AAA Authentication, page 10-11
- Configuring Switch-to-RADIUS-Server Communication, page 10-11
- Configuring the HTTP Server, page 10-13
- Configuring the Web-Based Authentication Parameters, page 10-15
- Removing Web-Based Authentication Cache Entries, page 10-16

Default Web-Based Authentication Configuration

Table 10-1 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>
<tr>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>None specified</td>
</tr>
<tr>
<td>UDP authentication port</td>
<td>1812</td>
</tr>
<tr>
<td>Key</td>
<td>None specified</td>
</tr>
<tr>
<td>Default value of inactivity timeout</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Enabled</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.
- You must configure the default ACL on the interface before configuring web-based authentication. Configure a port ACL for a Layer 2 interface or a Cisco IOS ACL for a Layer 3 interface.
- 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 is not supported for IPv6 traffic.

### Web-Based Authentication Configuration Task List

- Configuring the Authentication Rule and Interfaces, page 10-10
- Configuring AAA Authentication, page 10-11
- Configuring Switch-to-RADIUS-Server Communication, page 10-11
- Configuring the HTTP Server, page 10-13
- Configuring an AAA Fail Policy, page 10-15
- Configuring the Web-Based Authentication Parameters, page 10-15
- Removing Web-Based Authentication Cache Entries, page 10-16

### Configuring the Authentication Rule and Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>ip admission name name proxy http</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface type slot/port</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip access-group name</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip admission name</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip device tracking</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
<tr>
<td>Step 8</td>
<td>show ip admission configuration</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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 configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
  Auth-proxy name webauth1
    http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

### Configuring AAA Authentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>aaa new-model</td>
</tr>
<tr>
<td>Step 2</td>
<td>aaa authentication login default group {tacacs+</td>
</tr>
<tr>
<td>Step 3</td>
<td>aaa authorization auth-proxy default group {tacacs+</td>
</tr>
<tr>
<td>Step 4</td>
<td>tacacs-server host {hostname</td>
</tr>
<tr>
<td>Step 5</td>
<td>tacacs-server key {key-data}</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to enable AAA:

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group tacacs+
Switch(config)# aaa authorization auth-proxy default group tacacs+
```

### Configuring Switch-to-RADIUS-Server Communication

RADIUS security servers identification:
- 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.

To configure the RADIUS server parameters, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><em>ip radius source-interface interface_name</em></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>*radius-server host {hostname</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><em>radius-server key string</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><em>radius-server vsa send authentication</em></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><em>radius-server dead-criteria tries num-tries</em></td>
</tr>
</tbody>
</table>

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 retransmit*, and the *radius-server key* global configuration commands. For more information, see the Cisco IOS Security Configuration Guide, Release 12.2 and the Cisco IOS Security Command Reference, Release 12.2:

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.

This example shows how to configure the RADIUS server parameters on a switch:

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(config)# radius-server dead-criteria tries 2
```

### 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**
To ensure secure authentication when you enter the `ip http secure-secure` command, the login page is always in HTTPS (secure HTTP) even if the user sends an HTTP request.

- Customizing the Authentication Proxy Web Pages
- Specifying a Redirection URL for Successful Login

#### 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.

To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch flash memory, then perform this task in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td><code>ip admission proxy http login page file</code></td>
<td>Specify the location in the switch memory file system of the custom HTML file to use in place of the default login page. The <code>device:</code> is flash memory.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td><code>ip admission proxy http success page file</code></td>
<td>Specify the location of the custom HTML file to use in place of the default login success page.</td>
</tr>
</tbody>
</table>
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.

This example shows how to configure custom authentication proxy web pages:

```bash
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

This example shows how to verify the configuration of a custom authentication proxy web pages:

```bash
Switch# show ip admission configuration
Authentication proxy webpage
Login page       : flash:login.htm
Success page     : flash:success.htm
Fail Page        : flash:fail.htm
Login expired Page : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```
Specifying a Redirection URL for Successful Login

You can specify a URL to which the user is redirected after authentication, effectively replacing the internal *Success* HTML page.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip admission proxy http success redirect url-string</code></td>
<td>Specify a URL for redirection of the user in place of the default login success page.</td>
</tr>
</tbody>
</table>

When configuring a redirection URL for successful login, consider these guidelines:

- If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and is not available in the CLI. You can perform redirection in the custom-login success page.
- If the redirection URL feature is enabled, a configured auth-proxy-banner is not used.
- To remove the specification of a redirection URL, use the `no` form of the command.

This example shows how to configure a redirection URL for successful login:

```
Switch(config)# ip admission proxy http success redirect www.cisco.com
```

This example shows how to verify the redirection URL for successful login:

```
Switch# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Configuring the Web-Based Authentication Parameters

You can configure the maximum number of failed login attempts before the client is placed in a watch list for a waiting period.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>ip admission max-login-attempts number</code></td>
<td>Set the maximum number of failed login attempts. The range is 1 to 2147483647 attempts. The default is 5.</td>
</tr>
<tr>
<td>2</td>
<td><code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>3</td>
<td><code>show ip admission configuration</code></td>
<td>Display the authentication proxy configuration.</td>
</tr>
<tr>
<td>4</td>
<td><code>show ip admission cache</code></td>
<td>Display the list of authentication entries.</td>
</tr>
<tr>
<td>5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to set the maximum number of failed login attempts to 10:

```
Switch(config)# ip admission max-login-attempts 10
```
Configuring a Web Authentication Local Banner

Beginning in privileged EXEC mode, follow these steps to configure a local banner on a switch that has web authentication configured.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip admission auth-proxy-banner http [banner-text</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to configure a local banner with the custom message \textit{My Switch}:

\begin{verbatim}
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
\end{verbatim}

For more information about the \textbf{ip auth-proxy auth-proxy-banner} command, see the “Authentication Proxy Commands” section of the \textit{Cisco IOS Security Command Reference} on Cisco.com.

Removing Web-Based Authentication Cache Entries

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip auth-proxy cache {*</td>
<td>host ip address}</td>
</tr>
<tr>
<td>clear ip admission cache {*</td>
<td>host ip address}</td>
</tr>
</tbody>
</table>

This example shows how to remove the web-based authentication session for the client at the IP address 209.165.201.1:

\begin{verbatim}
Switch# clear ip auth-proxy cache 209.165.201.1
\end{verbatim}
Displaying Web-Based Authentication Status

Perform this task to display the web-based authentication settings for all interfaces or for specific ports:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;show authentication sessions [interface type slot/port]</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>
</tbody>
</table>

This example shows how to view only the global web-based authentication status:

```
Switch# show authentication sessions
```

This example shows how to view the web-based authentication settings for gigabit interface 3/27:

```
Switch# show authentication sessions interface gigabitethernet 3/27
```
Displaying Web-Based Authentication Status
Configuring Interface Characteristics

This chapter defines the types of Catalyst 3560 interfaces and describes how to configure them.

- Understanding Interface Types, page 11-1
- Using Interface Configuration Mode, page 11-11
- Configuring Ethernet Interfaces, page 11-15
- Configuring Layer 3 Interfaces, page 11-25
- Configuring the System MTU, page 11-28
- Monitoring and Maintaining the Interfaces, page 11-31

Note

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the Cisco IOS Interface Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software Release > 12.2 Mainline > Command References.

Understanding Interface Types

This section describes the different types of supported interfaces with references to chapters that contain more detailed information about configuring these interfaces.

- Port-Based VLANs, page 11-2
- Switch Ports, page 11-2
- Routed Ports, page 11-4
- Switch Virtual Interfaces, page 11-4
- EtherChannel Port Groups, page 11-6
- Dual-Purpose Uplink Ports, page 11-6
- Power over Ethernet Ports, page 11-6
- Connecting Interfaces, page 11-10
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. For more information about VLANs, see the Chapter 13, “Configuring VLANs.” 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 you configure a local port 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, you must first set VTP mode to transparent to configure extended-range VLANs (VLAN IDs 1006 to 4094). 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.
- For a tunnel port, set and define the VLAN ID for the customer-specific VLAN tag. See Chapter 16, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. You use switch ports for managing the physical interface and associated Layer 2 protocols. Switch ports do not handle routing or bridging.

A switch port can be an access port, a trunk port, or a tunnel 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. You must manually configure tunnel ports as part of an asymmetric link connected to an IEEE 802.1Q trunk port.

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

Use the `switchport` command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you change a Layer 3 interface into Layer 2 mode, the configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.</td>
</tr>
</tbody>
</table>

For detailed information about configuring access port and trunk port characteristics, see Chapter 13, “Configuring VLANs.” For more information about tunnel ports, see Chapter 16, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”
Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port.

If an access port receives a tagged packet (Inter-Switch Link [ISL] or IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

Supported access ports:
- Static access ports are manually assigned to a VLAN (or through a RADIUS server for use with IEEE 802.1x). For more information, see the “802.1x Authentication with VLAN Assignment” section on page 10-16.
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN. Traffic forwarding to and from the port is enabled only when the port VLAN membership 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 Catalyst 3560 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. For more information about voice VLAN ports, see Chapter 12, “Configuring Voice VLAN.”

Trunk Ports

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

These trunk port types are supported:
- In an ISL trunk port, all received packets are expected to be encapsulated with an ISL header, and all transmitted packets are sent with an ISL header. Native (non-tagged) frames received from an ISL trunk port are dropped.
- An 802.1Q trunk port supports simultaneous tagged and untagged traffic. An 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 affects only 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 enabled. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list, the trunk port automatically becomes a member of that VLAN. Traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of an enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and traffic for the VLAN is not forwarded to or from the port.

For more information about trunk ports, see Chapter 13, “Configuring VLANs.”

Tunnel Ports

Tunnel ports are used in IEEE 802.1Q tunneling to segregate the traffic of customers in a service-provider network from other customers who are using the same VLAN number. You configure an asymmetric link from a tunnel port on a service-provider edge switch to an IEEE 802.1Q trunk port.
on the customer switch. Packets entering the tunnel port on the edge switch, already IEEE 802.1Q-tagged with the customer VLANs, are encapsulated with another layer of an IEEE 802.1Q tag (called the metro tag), containing a VLAN ID unique in the service-provider network, for each customer. The double-tagged packets go through the service-provider network keeping the original customer VLANs separate from those of other customers. At the outbound interface, also a tunnel port, the metro tag is removed, and the original VLAN numbers from the customer network are retrieved.

Tunnel ports cannot be trunk ports or access ports and must belong to a VLAN unique to each customer.

For more information about tunnel ports, see Chapter 16, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

### 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. Routed ports are supported only on switches running the IP base or IP services image.

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. See the “Configuring Layer 3 Interfaces” section on page 11-25 for information about what happens when hardware resource limitations are reached.

For more information about IP unicast and multicast routing and routing protocols, see Chapter 37, “Configuring IP Unicast Routing” and Chapter 45, “Configuring IP Multicast Routing.”

**Note**

The IP base image supports static routing and the Routing Information Protocol (RIP). For full Layer 3 routing or for fallback bridging, you must have the IP services image installed.

### 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, to fallback-bridge nonroutable protocols 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.
You cannot delete interface VLAN 1.

SVIs provide IP host connectivity only to the system. In Layer 3 mode, you can configure routing across SVIs. Although the switch supports a total or 1005 VLANs (and SVIs), the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations. See the “Configuring Layer 3 Interfaces” section on page 11-25 for information about what happens when hardware resource limitations are reached.

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 encapsulated trunk port 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. For more information, see the “Manually Assigning IP Information” section on page 3-15.

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

SVIs support routing protocols and bridging configurations. For more information about configuring IP routing, see Chapter 37, “Configuring IP Unicast Routing,” Chapter 45, “Configuring IP Multicast Routing,” and Chapter 47, “Configuring Fallback Bridging.”

The IP base image supports static routing and RIP; for more advanced routing or for fallback bridging, you must have the IP services image installed.

SVI Autostate Exclude

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

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

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

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

The VLAN interface is brought up when one Layer 2 port in the VLAN has had time to converge (transition from STP listening-learning state to forwarding state). This prevents features such as routing protocols from using the VLAN interface as if it were fully operational and minimizes other problems, such as routing black holes. For information about configuring autostate exclude, see the “Configuring SVI Autostate Exclude” section on page 11-27.

**EtherChannel Port Groups**

EtherChannel port groups treat multiple switch ports as one switch port. An EtherChannel port group acts 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, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed port.

Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. The DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP) operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. Use the `channel-group interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together.

For Layer 3 interfaces, you manually create the logical interface by using the `interface port-channel global configuration command. Then you manually assign an interface to the EtherChannel by using the `channel-group interface configuration command.

For more information, see Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

**Dual-Purpose Uplink Ports**

Some switches support dual-purpose uplink ports. Each uplink port is considered as a single interface with dual front ends—an RJ-45 connector and a small form-factor pluggable (SFP) module connector. The dual front ends are not redundant interfaces, and the switch activates only one connector of the pair.

By default, the switch dynamically selects the interface type that first links up. However, you can use the `media-type interface configuration command to manually select the RJ-45 connector or the SFP module connector. For information about configuring speed and duplex settings for a dual-purpose uplink, see the “Setting the Interface Speed and Duplex Parameters” section on page 11-19.

Each uplink port has two LEDs: one shows the status of the RJ-45 port, and one shows the status of the SFP module port. The port LED is on for whichever connector is active. For more information about the LEDs, see the hardware installation guide.

**Power over Ethernet Ports**

PoE switch ports automatically supply power to these connected devices (if the switch senses that there is no power on the circuit):
- Cisco pre-standard powered devices (such as Cisco IP Phones and Cisco Aironet access points)
- IEEE 802.3 af-compliant powered devices

A powered device can receive redundant power when it is connected only to a PoE switch port and to an AC power source. This section has this PoE information:

- Supported Protocols and Standards, page 11-7
- Powered-Device Detection and Initial Power Allocation, page 11-7
- Power Management Modes, page 11-9

### 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 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.

Before Cisco IOS Release 12.2(25)SE, PoE-capable switches (without intelligent power management support) caused high-power powered devices that supported intelligent power management to operate in low-power mode. Devices in low-power mode are not fully functional.

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:

- A Cisco pre-standard powered device does not provide its power requirement when the switch detects it, so the switch allocates 15.4 W as the initial allocation for power budgeting.

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 11-1 lists these levels.

**Table 11-1 IEEE Power Classifications**

<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 (reserved for future use)</td>
<td>Treat as Class 0</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 actual power consumption requirement of the connected Cisco powered devices, and 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.

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

Supported 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 needs more than the maximum wattage, the powered device is shutdown.

  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 power is never applied to a PoE-capable port, making the port a data-only port.

For information on configuring a PoE port, see the “Configuring a Power Management Mode on a PoE Port” section on page 11-22.
Connecting Interfaces

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

With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router. By using the switch with routing enabled, when you configure both VLAN 20 and VLAN 30 with an SVI to which an IP address is assigned, packets can be sent from Host A to Host B directly through the switch with no need for an external router (Figure 11-1).

Figure 11-1 Connecting VLANs with a Layer 3 Switch

With the IP services image, the switch supports two methods of forwarding traffic between interfaces: routing and fallback bridging. With the IP base image, only basic routing (static routing and RIP) is supported. Whenever possible, to maintain high performance, forwarding is done by the switch hardware. However, only IP Version 4 packets with Ethernet II encapsulation can be routed in hardware. Non-IP traffic and traffic with other encapsulation methods can be fallback-bridged by hardware.

- The routing function can be enabled on all SVIs and routed ports. The switch routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI or routed port, any IP traffic received from these ports is routed. For more information, see Chapter 37, “Configuring IP Unicast Routing,” Chapter 45, “Configuring IP Multicast Routing,” and Chapter 46, “Configuring MSDP.”

- Fallback bridging forwards traffic that the switch does not route or traffic belonging to a nonroutable protocol, such as DECnet. Fallback bridging connects multiple VLANs into one bridge domain by bridging between two or more SVIs or routed ports. When configuring fallback bridging, you assign SVIs or routed ports to bridge groups with each SVI or routed port assigned to only one bridge group. All interfaces in the same group belong to the same bridge domain. For more information, see Chapter 47, “Configuring Fallback Bridging.”
Using 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 (see the “Configuring a Range of Interfaces” section on page 11-12).

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

- **Type**—Port types depend on those supported on the switch. Possible types are: Fast Ethernet (fastethernet or fa) for 10/100 Mb/s Ethernet, Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mb/s Ethernet ports, 10-Gigabit Ethernet (tengigabitethernet or te) for 10,000 Mb/s, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces.
- **Module number**—The module or slot number on the switch (always 0).
- **Port number**—The interface number on the switch. The port numbers always begin at 1, starting with the far left port when facing the front of the switch, for example, fastethernet0/1 or gigabitethernet0/1. If there is more than one interface type (for example, 10/100 ports and SFP module ports, the port numbers restart with the second interface type: gigabitethernet0/1. 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 looking at the switch. You can also use the `show` privileged EXEC commands to display information about a specific interface or all the interfaces. The remainder of this chapter primarily provides physical interface configuration procedures.

This example identifies an interface:

- To configure 10/100/1000 port 4, enter this command:
  ```
  Switch(config)# interface gigabitethernet0/4
  ```

**Note** Configuration examples and outputs in this book might not be specific to your switch, particularly regarding the presence of a stack member number.

Procedures for Configuring Interfaces

These general instructions apply to all interface configuration processes.

**Step 1** Enter the `configure terminal` command at the privileged EXEC prompt:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

**Step 2** Enter the `interface` global configuration command.

Identify the interface type and the interface number, Gigabit Ethernet port 1 in this example:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)#
```
### Configuring Interface Characteristics

**Using Interface Configuration Mode**

**Step 3** Follow each `interface` command with the configuration commands that the interface requires. The commands that you enter define the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter `end` to return to privileged EXEC mode.

You can also configure a range of interfaces by using the `interface range` or `interface range macro` global configuration commands. Interfaces configured in a range must be the same type and must be configured with the same feature options.

**Step 4** After you configure an interface, verify its status by using the `show` privileged EXEC commands listed in the “Monitoring and Maintaining the Interfaces” section on page 11-31.

Enter the `show interfaces` privileged EXEC command to see 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.

### Configuring a Range of Interfaces

You can use the `interface range` global configuration command to configure multiple interfaces with the same configuration parameters. 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.

Beginning in privileged EXEC mode, follow these steps to configure a range of interfaces with the same parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`interface range {port-range</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><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show interfaces [interface-id]</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
When using the **interface range** global configuration command, note these guidelines:

- **Valid entries for** `port-range`, depending on port types on the switch:
  - `vlan vlan-ID - vlan-ID`, where the VLAN ID is 1 to 4094
  - ``, where the module is always 0
  - `fastethernet module/{first port} - {last port}`, where the module is always 0
  - `gigabitethernet module/{first port} - {last port}`, where the module is always 0
  - `port-channel port-channel-number - port-channel-number`, where the `port-channel-number` is 1 to 48

  **Note** When you use the **interface range** command with port channels, the first and last port-channel number must be active port channels.

- You must add a space between the first interface number and the hyphen when using the `interface range` command.
  
  For example, `interface range gigabitethernet 0/1 - 4` is a valid range; `interface range gigabitethernet0/1-4` is not.

- The **interface range** command only works with VLAN interfaces that have been configured with the `interface vlan` command. The `show running-config` privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the `show running-config` command cannot be used with the `interface range` command.

- All interfaces defined in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs), but you can enter multiple ranges in a command.

This example shows how to use the **interface range** global configuration command to set the speed on ports 1 to 2 to 100 Mb/s:

```sh
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)# speed 100
```

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

```sh
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 3, gigabitethernet0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

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

**Configuring and Using Interface Range Macros**

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.
Beginning in privileged EXEC mode, follow these steps to define an interface-range macro:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>define interface-range macro_name</td>
<td>Define the interface-range macro, and save it in NVRAM.</td>
</tr>
<tr>
<td></td>
<td>• The macro_name is a 32-character maximum character string.</td>
</tr>
<tr>
<td></td>
<td>• A macro can contain up to five comma-separated interface ranges.</td>
</tr>
<tr>
<td></td>
<td>• Each interface-range must consist of the same port type.</td>
</tr>
<tr>
<td>interface range macro macro_name</td>
<td>Select the interface range to be configured using the values saved in the interface-range macro called macro_name.</td>
</tr>
<tr>
<td></td>
<td>You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>include define</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no define interface-range macro_name global configuration command to delete a macro.

When using the define interface-range global configuration command, note these guidelines:

- Valid entries for interface-range, depending on port types on the switch:
  - vlan vlan-ID - vlan-ID, where the VLAN ID is 1 to 4094
  - fastethernet module/{first port} - {last port}, where the module is always 0
  - gigabitethernet module/{first port} - {last port}, where the module is always 0
  - port-channel port-channel-number - port-channel-number, where the port-channel-number is 1 to 48

  **Note** When you use the interface range command with port channels, the first and last port-channel number must be active port channels.

- You must add a space between the first interface number and the hyphen when entering an interface-range.
  
  For example, gigabitethernet 0/1 - 4 is a valid range; gigabitethernet 0/1-4 is not.

- The VLAN interfaces must have been configured with the interface vlan command. The show running-config privileged EXEC command displays the configured VLAN interfaces. VLAN interfaces not displayed by the show running-config command cannot be used as interface-ranges.

- All interfaces defined as in a range must be the same type (all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs), but you can combine multiple interface types in a macro.

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

```bash
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet0/1 - 2
Switch(config)# end
Switch# show running-config | include define
```
Switch# define interface-range enet_list gigabitethernet0/1 - 2

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

Switch# configure terminal
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
Switch(config)# end

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

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

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

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

Configuring Ethernet Interfaces

These sections contain this configuration information:

- Default Ethernet Interface Configuration, page 11-15
- Setting the Type of a Dual-Purpose Uplink Port, page 11-17
- Configuring Interface Speed and Duplex Mode, page 11-18
- Configuring IEEE 802.3x Flow Control, page 11-20
- Configuring Auto-MDIX on an Interface, page 11-21
- Configuring a Power Management Mode on a PoE Port, page 11-22
- Budgeting Power for Devices Connected to a PoE Port, page 11-23
- Adding a Description for an Interface, page 11-25

Default Ethernet Interface Configuration

Table 11-2 shows the Ethernet interface default configuration. For more details on the VLAN parameters listed in the table, see Chapter 13, “Configuring VL ANs.” For details on controlling traffic to the port, see Chapter 23, “Configuring Port-Based Traffic Control.”

**Note**

To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the `switchport` 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.
### Table 11-2  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 (switchport command).</td>
</tr>
<tr>
<td>Allowed VLAN range</td>
<td>VLANs 1 to 4094.</td>
</tr>
<tr>
<td>Default VLAN (for access ports)</td>
<td>VLAN 1 (Layer 2 interfaces only).</td>
</tr>
<tr>
<td>Native VLAN (for IEEE 802.1Q trunks)</td>
<td>VLAN 1 (Layer 2 interfaces only).</td>
</tr>
<tr>
<td>VLAN trunking</td>
<td>Switchport mode dynamic auto (supports DTP) (Layer 2 interfaces only).</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.</td>
</tr>
<tr>
<td>Duplex mode</td>
<td>Autonegotiate.</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control is set to receive: off. It is always off for sent packets.</td>
</tr>
<tr>
<td>EtherChannel (PAgP)</td>
<td>Disabled on all Ethernet ports. Chapter 35, “Configuring EtherChannels and Link-State Tracking.”</td>
</tr>
<tr>
<td>Port blocking (unknown multicast and unknown unicast traffic)</td>
<td>Disabled (not blocked) (Layer 2 interfaces only). See the “Configuring Port Blocking” section on page 23-8.</td>
</tr>
<tr>
<td>Broadcast, multicast, and unicast storm control</td>
<td>Disabled. See the “Default Storm Control Configuration” section on page 23-3.</td>
</tr>
<tr>
<td>Protected port</td>
<td>Disabled (Layer 2 interfaces only). See the “Configuring Protected Ports” section on page 23-6.</td>
</tr>
<tr>
<td>Port security</td>
<td>Disabled (Layer 2 interfaces only). See the “Default Port Security Configuration” section on page 23-11.</td>
</tr>
<tr>
<td>Port Fast</td>
<td>Disabled. See the “Default Optional Spanning-Tree Configuration” section on page 18-10.</td>
</tr>
<tr>
<td>Auto-MDIX</td>
<td>Enabled. The switch might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the switch through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port.</td>
</tr>
<tr>
<td>Power over Ethernet (PoE)</td>
<td>Enabled (auto).</td>
</tr>
<tr>
<td>Keepalive messages</td>
<td>Disabled on SFP module ports; enabled on all other ports.</td>
</tr>
</tbody>
</table>

### Setting the Type of a Dual-Purpose Uplink Port

Some switches support dual-purpose uplink ports. By default, the switch dynamically selects the interface type that first links up. However, you can use the media-type interface configuration command to manually select the RJ-45 connector or the SFP module connector. For more information, see the...
“Dual-Purpose Uplink Ports” section on page 11-6.
Beginning in privileged EXEC mode, follow these steps to select which dual-purpose uplink to activate so that you can set the speed and duplex. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</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> interface interface-id</td>
<td>Specify the dual-purpose uplink port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> media-type {auto-select</td>
<td>rj45</td>
</tr>
<tr>
<td>auto-select — The switch dynamically selects the type. When link up is achieved, the switch disables the other type until the active link goes down. When the active link goes down, the switch enables both types until one of them links up. In auto-select mode, the switch configures both types with autonegotiation of speed and duplex (the default). Depending on the type of installed SFP module, the switch might not be able to dynamically select it. For more information, see the information that follows this procedure.</td>
<td></td>
</tr>
<tr>
<td>rj45 — The switch disables the SFP module interface. If you connect an SFP module to this port, it cannot attain a link even if the RJ-45 side is down or is not connected. In this mode, the dual-purpose port behaves like a 10/100/1000BASE-TX interface. You can configure the speed and duplex settings consistent with this interface type.</td>
<td></td>
</tr>
<tr>
<td>sfp — The switch disables the RJ-45 interface. If you connect a cable to the RJ-45 port, it cannot attain a link even if the SFP module side is down or if the SFP module is not present. Based on the type of installed SFP module, you can configure the speed and duplex settings consistent with this interface type.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show interfaces interface-id transceiver properties</td>
<td>Verify your setting.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **media-type auto interface** or the **no media-type** interface configuration commands.

The switch configures both types to autonegotiate speed and duplex (the default). If you configure **auto-select**, you cannot configure the **speed** and **duplex** interface configuration commands.

When the switch powers on or when you enable a dual-purpose uplink port through the **shutdown** and the **no shutdown** interface configuration commands, the switch gives preference to the SFP module interface. In all other situations, the switch selects the active link based on which type first links up.
Configuring Interface Speed and Duplex Mode

Depending on the supported port types, Ethernet interfaces on the switch operate at 10, 100, or 1000 Mb/s, or 10,000 Mb/s and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mb/s ports operate in half-duplex mode, which means that stations can either receive or send traffic.

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

These sections describe how to configure the interface speed and duplex mode:

- Speed and Duplex Configuration Guidelines, page 11-18
- Setting the Interface Speed and Duplex Parameters, page 11-19

Speed and Duplex Configuration Guidelines

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

- Fast Ethernet (10/100-Mb/s) ports support all speed and duplex options.
- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.
- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
  - The 1000BASE-x (where -x is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the nonegotiate keyword in the speed interface configuration command. Duplex options are not supported.
  - The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.
  - The 100BASE-x (where -x is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support only 100 Mb/s. These modules support full- and half-duplex options but do not support autonegotiation.

For information about which SFP modules are supported on your switch, see the product release notes.

- 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.

Caution

Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.
Setting the Interface Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex mode for a physical interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>speed {10</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>duplex {auto</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show interfaces interface-id</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no speed and no duplex interface configuration commands to return the interface to the default speed and duplex settings (autonegotiate). To return all interface settings to the defaults, use the default interface interface-id interface configuration command.

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

Switch# configure terminal
Switch(config)# interface fasttethernet0/3
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 gigabitethernet0/2
Switch(config-if)# speed 100
```

## Configuring 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**

Ports on the switch 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.

**Note**

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

Beginning in privileged EXEC mode, follow these steps to configure flow control on an interface:

<table>
<thead>
<tr>
<th>Command</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> interface interface-id</td>
<td>Specify the physical interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> flowcontrol {receive} {on</td>
<td>off</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show interfaces interface-id</td>
<td>Verify the interface flow control settings.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable flow control, use the `flowcontrol receive off` interface configuration command.

This example shows how to turn on flow control on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive on
Switch(config-if)# end
```
Configuring 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.

Auto-MDIX is enabled by default. When you enable auto-MDIX, you must also set the interface speed and duplex to auto so that the feature operates correctly.

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

Table 11-3 shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

<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>

Starting in privileged EXEC mode, follow these steps to configure auto-MDIX on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the physical interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 speed auto</td>
<td>Configure the interface to autonegotiate speed with the connected device.</td>
</tr>
<tr>
<td>Step 4 duplex auto</td>
<td>Configure the interface to autonegotiate duplex mode with the connected device.</td>
</tr>
<tr>
<td>Step 5 mdix auto</td>
<td>Enable auto-MDIX on the interface.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show controllers ethernet-controller interface-id phy</td>
<td>Verify the operational state of the auto-MDIX feature on the interface.</td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable auto-MDIX, use the no mdix auto interface configuration command.

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

Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end

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

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

**Note**
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.

Beginning in privileged EXEC mode, follow these steps to configure a power management mode on a PoE-capable port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Specify the physical port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>power inline {auto [max max-wattage]</td>
</tr>
</tbody>
</table>
| | Configure the PoE mode on the port. The keywords have these meanings:
| | • **auto**—Enable powered-device detection. If enough power is available, automatically allocate power to the PoE port after device detection. This is the default setting.
| | • (Optional) **max max-wattage**—Limit the power allowed on the port. The range is 4000 to 15400 milliwatts. If no value is specified, the maximum is allowed (15400 milliwatts).
| | • **never**—Disable 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 an error-disabled state.
| | • **static**—Enable powered-device detection. Pre-allocate (reserve) power for a port before the switch discovers the powered device. The switch reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection.
| The switch allocates power to a port configured in static mode before it allocates power to a port configured in auto mode. |
| **Step 4** | end |
| | Return to privileged EXEC mode. |
Chapter 11 Configuring Interface Characteristics

### Configuring Ethernet Interfaces

For information about the output of the `show power inline` EXEC command, see the command reference for this release. For more information about PoE-related commands, see the “Troubleshooting Power over Ethernet Switch Ports” section on page 48-11. For information about configuring voice VLAN, see Chapter 12, “Configuring Voice VLAN.”

### 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) to determine the *actual* power consumption of the devices, and the switch adjusts the power budget accordingly. The CDP protocol works with Cisco powered devices and 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 milliwatts for the device, regardless of the actual amount of power needed. If the powered device reports a higher class than its actual 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` 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.

For example, if the switch budgets 15,400 milliwatts on each PoE port, you can connect only 24 Class 0 powered devices. If your Class 0 device power requirement is actually 5000 milliwatts, you can set the consumption wattage to 5000 milliwatts and connect up to 48 devices. The total PoE output power available on a 24-port or 48-port switch is 370,000 milliwatts.

**Caution**

You should carefully plan your switch power budget 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.

When you enter the `power inline consumption default wattage` or the `no power inline consumption default` global configuration command, or the `power inline consumption wattage` or the `no power inline consumption` interface configuration command this caution message appears:

```plaintext
%CAUTION: Interface interface-id: 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. Refer to documentation.
```

If the power supply is over-subscribed to by up to 20 percent, the switch continues to operate but its reliability is reduced. If the power supply is subscribed to by more than 20 percent, the short-circuit protection circuitry triggers and shuts the switch down.

---

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show power inline [interface-id]</code></td>
<td>Display PoE status for a switch or for the specified interface.</td>
</tr>
</tbody>
</table>

**Step 6**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
For more information about the IEEE power classifications, see the “Power over Ethernet Ports” section on page 11-6.

Beginning in privileged EXEC mode, follow these steps to configure the amount of power budgeted to a powered device connected to each PoE port on a switch:

<table>
<thead>
<tr>
<th>Command</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> no cdp run</td>
<td>(Optional) Disable CDP.</td>
</tr>
<tr>
<td><strong>Step 3</strong> power inline consumption default</td>
<td>Configure the power consumption of powered devices connected to each PoE port on the switch.</td>
</tr>
<tr>
<td>wattage</td>
<td>The range for each device is 4000 to 15400 milliwatts. The default is 15400 milliwatts.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you use this command, we recommend you also enable power policing.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show power inline consumption</td>
<td>Display the power consumption status.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no power inline consumption default** global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure amount of power budgeted to a powered device connected to a specific PoE port:

<table>
<thead>
<tr>
<th>Command</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> no cdp run</td>
<td>(Optional) Disable CDP.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specify the physical port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> power inline consumption wattage</td>
<td>Configure the power consumption of a powered device connected to a PoE port on the switch.</td>
</tr>
<tr>
<td></td>
<td>The range for each device is 4000 to 15400 milliwatts. The default is 15400 milliwatts.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you use this command, we recommend you also enable power policing.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show power inline consumption</td>
<td>Display the power consumption status.</td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no power inline consumption** interface configuration command.

For information about the output of the **show power inline consumption** privileged EXEC command, see the command reference for this release.
Chapter 11 Configuring Interface Characteristics

Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of these privileged EXEC commands: `show configuration`, `show running-config`, and `show interfaces`.

Beginning in privileged EXEC mode, follow these steps to add a description for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</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>2</td>
<td><code>interface interface-id</code></td>
<td>Specify the interface for which you are adding a description, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td><code>description string</code></td>
<td>Add a description (up to 240 characters) for an interface.</td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td><code>show interfaces interface-id description</code> or <code>show running-config</code></td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>6</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no description` interface configuration command to delete the description.

This example shows how to add a description on a port and how to verify the description:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# description Connects to Marketing
Switch(config-if)# end
Switch# show interfaces gigabitethernet0/2 description
Interface Status     Protocol Description
Gi0/2    admin down     down    Connects to Marketing
```

Configuring Layer 3 Interfaces

The switch supports these types of Layer 3 interfaces:

- **SVIs:** You should configure SVIs for any VLANs for which you want to route traffic. SVIs are created when you enter a VLAN ID following the `interface vlan` global configuration command. To delete an SVI, use the `no interface vlan` global configuration command. You cannot delete interface VLAN 1.

  **Note** When you create an SVI, it does not become active until it is associated with a physical port. For information about assigning Layer 2 ports to VLANs, see Chapter 13, “Configuring VLANs.”

When configuring SVIs, you can also configure SVI autostate exclude on a port in the SVI to exclude that port from being included in determining SVI line-state status. See the “Configuring SVI Autostate Exclude” section on page 11-27.
11-26

Chapter 11  Configuring Interface Characteristics

- Routed ports: Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.

- Layer 3 EtherChannel ports: EtherChannel interfaces made up of routed ports.
  EtherChannel port interfaces are described in Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

A Layer 3 switch can have an IP address assigned to each routed port and SVI.

There is no defined limit to the number of SVIs and routed ports that can be configured in a switch. However, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might have an impact on CPU usage because of hardware limitations. If the switch is using maximum hardware resources, attempts to create a routed port or SVI have these results:

- If you try to create a new routed port, the switch generates a message that there are not enough resources to convert the interface to a routed port, and the interface remains as a switchport.

- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.

- If the switch is notified by VLAN Trunking Protocol (VTP) of a new VLAN, 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.

- If the switch attempts to boot up with a configuration that has more VLANs and routed ports than hardware can support, the VLANs are created, but the routed ports are shut down, and the switch sends a message that this was due to insufficient hardware resources.

All Layer 3 interfaces require an IP address to route traffic. This procedure shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface.

**Note** If the physical port is in Layer 2 mode (the default), you must enter the **no switchport** interface configuration command to put the interface into Layer 3 mode. Entering a **no switchport** command disables and then re-enables the interface, which might generate messages on the device to which the interface is connected. Furthermore, 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, and the interface is returned to its default configuration.

Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface {{ fastethernet</td>
</tr>
<tr>
<td>Step 3</td>
<td>no switchport</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip address ip_address subnet_mask</td>
</tr>
<tr>
<td>Step 5</td>
<td>no shutdown</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
</tbody>
</table>
To remove an IP address from an interface, use the `no ip address` interface configuration command.

This example shows how to configure a port as a routed port and to assign it an IP address:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
Switch(config-if)# no shutdown
```

### Configuring SVI Autostate Exclude

Configuring SVI autostate exclude on an access or trunk port in an SVI excludes that port in the calculation of the status of the SVI (up or down line state) even if it belongs to the same VLAN. When the excluded port is in the up state, and all other ports in the VLAN are in the down state, the SVI state is changed to down.

At least one port in the VLAN should be up and not excluded to keep the SVI line state up. You can use this command to exclude the monitoring port status when determining the status of the SVI.

Beginning in privileged EXEC mode, follow these steps to exclude a port from SVI state-change calculations:

```
Step 1  configure terminal
       Enter global configuration mode.

Step 2  interface interface-id
       Specify a Layer 2 interface (physical port or port channel), and enter interface configuration mode.

Step 3  switchport autostate exclude
       Exclude the access or trunk port when defining the status of an SVI line state (up or down)

Step 4  end
       Return to privileged EXEC mode.

Step 5  show running config interface interface-id
       (Optional) Show the running configuration.

Step 6  show interface interface-id switchport
       Verify the configuration.

Step 7  copy running-config startup-config
       (Optional) Save your entries in the configuration file.
```

This example shows how to configure an access or trunk port in an SVI to be excluded from the status calculation:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport autostate exclude
Switch(config-if)# exit
```
Configuring the System MTU

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

You can change the MTU size for routed ports by using the `system mtu routing` global configuration command.

**Note**

You cannot configure a routing MTU size that exceeds the system MTU size. If you change the system MTU size to a value smaller than the currently configured routing MTU size, the configuration change is accepted, but not applied until the next switch reset. When the configuration change takes effect, the routing MTU size automatically defaults to the new system MTU size.

Gigabit Ethernet ports are not affected by the `system mtu` command; 10/100 ports are not affected by the `system mtu jumbo` command. If you do not configure the `system mtu jumbo` command, the setting of the `system mtu` command applies to all Gigabit Ethernet interfaces.

You cannot set the MTU size for an individual interface; you set it for all 10/100 or all Gigabit Ethernet interfaces. When you change the system or jumbo MTU size, you must reset the switch before the new configuration takes effect. The `system mtu routing` command does not require a switch reset to take effect.

Frames sizes that can be received by the switch CPU are limited to 1998 bytes, no matter what value was entered with the `system mtu` or `system mtu jumbo` commands. Although frames that are forwarded or routed are typically not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, SNMP, Telnet, or routing protocols.

Routed packets are subjected to MTU checks on the output ports. The MTU value used for routed ports is derived from the applied `system mtu` value (not the `system mtu jumbo` value). That is, the routed MTU is never greater than the system MTU for any VLAN. The routing protocols use the system MTU value when negotiating adjacencies and the MTU of the link. For example, the Open Shortest Path First (OSPF) protocol uses this MTU value before setting up an adjacency with a peer router. To view the MTU value for routed packets for a specific VLAN, use the `show platform port-asic mvid` privileged EXEC command.

**Note**

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>system mtu bytes</code></td>
<td>(Optional) Change the MTU size for all interfaces on the switch that are operating at 10 or 100 Mb/s. The range is 1500 to 1998 bytes; the default is 1500 bytes.</td>
</tr>
</tbody>
</table>
If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

Once the switch reloads, you can verify your settings by entering the `show system mtu` privileged EXEC command.

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

This example shows the response when you try to set Gigabit Ethernet interfaces to an out-of-range number:

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

### Configuring the Cisco Redundant Power System 2300

Follow these guidelines:

- The RPS name is a 16-character-maximum string.
- On a Catalyst 3560v2 switch, the RPS name applies to the connected RPS 2300.
- If you do not want the RPS 2300 to provide power to a switch, but do not want to disconnect the cable between the switch and the RPS 2300, use the `power rps switch-number port rps-port-id mode standby` user EXEC command.
- You can configure the priority of an RPS 2300 port from 1 to 6. A value of 1 assigns highest priority to a port and its connected device. A value of 6 assigns lowest priority to a port and its connected device.

If multiple switches connected to the RPS 2300 need power, the RPS 2300 powers those with the highest priority. It applies any other available power to the lower-priority switches.
Beginning in user EXEC mode:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`power rps name {string</td>
<td>Specify the name of the RPS 2300.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>serialnumber}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>name</code>—Set the name of the RPS 2300, and enter one of these options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>string</code>—Specify the name, such as <code>port1</code> or “port 1”. Using</td>
</tr>
<tr>
<td></td>
<td></td>
<td>quotation marks before and after the name is optional, but you</td>
</tr>
<tr>
<td></td>
<td></td>
<td>must use quotation marks if you want to include spaces in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>port name. The name can have up to 16 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>serialnumber</code>—Configure the switch to use the RPS 2300 serial</td>
</tr>
<tr>
<td></td>
<td></td>
<td>number as the name.</td>
</tr>
<tr>
<td>Step 2</td>
<td>`power rps port rps-port-id mode {active</td>
<td>Specify the mode of the RPS 2300 port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>standby}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>port rps-port-id</code>—Specify the RPS 2300 port. The range is from 1 to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>mode</code>—Set the mode of the RPS 2300 port:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>active</code>—The RPS 2300 can provide the power to a switch when the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>switch internal power supply cannot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>standby</code>—The RPS 2300 is not providing power to a switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default mode for RPS ports is <code>active</code>.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>power rps priority priority</code></td>
<td>Set the priority of the RPS 2300 port. The range is from 1 to 6,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>where 1 is the highest priority and 6 is the lowest priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default port priority is 6.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show env rps</code></td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default name setting (no configured name), use the `power rps port rps-port-id name` user EXEC command with no space between the quotation marks.

To return to the default port mode, use the `power rps port rps-port-id active` command.

To return to the default port priority, use the `power rps port rps-port-id priority` command.

For more information about using the `power rps` user EXEC command, see the command reference for this release.
Monitoring and Maintaining the Interfaces

These sections contain interface monitoring and maintenance information:

- Monitoring Interface Status, page 11-31
- Clearing and Resetting Interfaces and Counters, page 11-32
- Shutting Down and Restarting the Interface, page 11-33

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 11-4 lists some of these interface monitoring commands. (You can display the full list of show commands by using the show ? command at the privileged EXEC prompt.) These commands are fully described in the Cisco IOS Interface Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show env rps</td>
<td>(Optional) Display any connected redundant power system.</td>
</tr>
<tr>
<td>show interfaces [interface-id]</td>
<td>(Optional) Display the status and configuration of all interfaces or a specific interface.</td>
</tr>
<tr>
<td>show interfaces interface-id status [err-disabled]</td>
<td>(Optional) Display interface status or a list of interfaces in an error-disabled state.</td>
</tr>
<tr>
<td>show interfaces [interface-id] switchport</td>
<td>(Optional) Display administrative and operational status of switching 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>(Optional) Display the description configured on an interface or all interfaces and the interface status.</td>
</tr>
<tr>
<td>show ip interface [interface-id]</td>
<td>(Optional) Display 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>(Optional) Display the input and output packets by the switching path for the interface.</td>
</tr>
<tr>
<td>show interfaces transceiver properties</td>
<td>(Optional) Display speed, duplex, and inline power settings on the interface.</td>
</tr>
<tr>
<td>show interfaces transceiver detail</td>
<td>(Optional) Display temperature, voltage, or amount of current on the interface.</td>
</tr>
<tr>
<td>show interfaces [interface-id] [transceiver properties</td>
<td>[transceiver properties</td>
</tr>
</tbody>
</table>

Table 11-4  Show Commands for Interfaces
Table 11-4   Show Commands for Interfaces (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show running-config interface [interface-id]</td>
<td>Display the running configuration in RAM for the interface.</td>
</tr>
<tr>
<td>show version</td>
<td>Display the hardware configuration, software version, the names and sources of configuration files, and the boot images.</td>
</tr>
<tr>
<td>show controllers ethernet-controller interface-id phy</td>
<td>Display the operational state of the auto-MDIX feature on the interface.</td>
</tr>
<tr>
<td>show power inline [interface-id]</td>
<td>Display PoE status for a switch or for an interface.</td>
</tr>
</tbody>
</table>

Clearing and Resetting Interfaces and Counters

Table 11-5 lists the privileged EXEC mode clear commands that you can use to clear counters and reset interfaces.

Table 11-5   Clear Commands for Interfaces

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

To clear the interface counters shown by the show interfaces privileged EXEC command, use the clear counters privileged EXEC command. The clear counters command clears all current interface counters from the interface unless you specify optional arguments that clear only a specific interface type from a specific interface number.

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.
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.

Beginning in privileged EXEC mode, follow these steps to shut down an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface { vlan vlan-id</td>
<td>{ fastethernet</td>
</tr>
<tr>
<td>3</td>
<td>shutdown</td>
<td>Shut down an interface.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Verify your entry.</td>
</tr>
</tbody>
</table>
Chapter 13

Configuring VLANs

This chapter describes how to configure normal-range VLANs (VLAN IDs 1 to 1005) and extended-range VLANs (VLAN IDs 1006 to 4094) on the Catalyst 3560 switch. It includes information about VLAN membership modes, VLAN configuration modes, VLAN trunks, and dynamic VLAN assignment from a VLAN Membership Policy Server (VMPS).

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter consists of these sections:

- Understanding VLANs, page 13-1
- Configuring Normal-Range VLANs, page 13-4
- Configuring Extended-Range VLANs, page 13-11
- Displaying VLANs, page 13-15
- Configuring VLAN Trunks, page 13-16
- Configuring VMPS, page 13-28

Understanding VLANs

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, as shown in Figure 13-1. 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. See Chapter 26, “Configuring STP.”

Note

Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration for your network. For more information on VTP, see Chapter 14, “Configuring VTP.”
Figure 13-1 shows an example of VLANs segmented into logically defined networks.

**Figure 13-1 VLANs as Logically Defined Networks**

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 or fallback bridged. 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. For more information, see the “Switch Virtual Interfaces” section on page 11-4 and the “Configuring Layer 3 Interfaces” section on page 11-25.

**Note**

If you plan to configure many VLANs on the switch and to not enable routing, you can use the `sdm prefer vlan` global configuration command to set the Switch Database Management (sdm) feature to the VLAN template, which configures system resources to support the maximum number of unicast MAC addresses. For more information on the SDM templates, see Chapter 7, “Configuring SDM Templates,” or see the `sdm prefer` command in the command reference for this release.

**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 supports a total of 1005 (normal range and extended range) VLANs, the number of routed ports, SVIs, and other 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 128 spanning-tree instances. One spanning-tree instance is allowed per VLAN. See the “Normal-Range VLAN Configuration Guidelines” section on page 13-6 for more information about the number of spanning-tree instances and the number of VLANs. The switch supports both Inter-Switch Link (ISL) and 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. Table 13-1 lists the membership modes and membership and VTP 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. For more information, see the “Assigning Static-Access Ports to a VLAN” section on page 13-9.</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 (ISL or 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. For information about configuring trunk ports, see the “Configuring an Ethernet Interface as a Trunk Port” section on page 13-19.</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 VMPS. The VMPS can be a Catalyst 5000 or Catalyst 6500 series switch, for example, but never a Catalyst 3560 switch. The Catalyst 3560 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. For configuration information, see the “Configuring Dynamic-Access Ports on VMPS Clients” section on page 13-31.</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>
</tbody>
</table>
Configuring Normal-Range VLANs

Normal-range VLANs are VLANs with VLAN IDs 1 to 1005. 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.)

In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create extended-range VLANs (VLANs with IDs from 1006 to 4094), but these VLANs are not saved in the VLAN database. VTP version 3 supports extended-range VLANs in VTP server and transparent mode. See the “Configuring Extended-Range VLANs” section on page 13-11.

Configurations for VLAN IDs 1 to 1005 are written to the file vlan.dat (VLAN database), and you can display them by entering the show vlan privileged EXEC command. The vlan.dat file is stored in flash memory.

---

### Table 13-1  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>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. For more information about voice VLAN ports, see Chapter 12, “Configuring Voice VLAN.”</td>
<td>VTP is not required; it has no effect on a voice VLAN.</td>
</tr>
<tr>
<td>Private VLAN</td>
<td>A private VLAN port is a host or promiscuous port that belongs to a private VLAN primary or secondary VLAN. For information about private VLANs, see Chapter 15, “Configuring Private VLANs.”</td>
<td>In VTP versions 1 and 2, the switch must be in VTP transparent mode when you configure private VLANs. When private VLANs are configured on the switch, do not change VTP mode from transparent to client or server mode. VTP version 3 supports private VLANs in any mode.</td>
</tr>
<tr>
<td>Tunnel (dot1q-tunnel)</td>
<td>Tunnel ports are used for IEEE 802.1Q tunneling to maintain customer VLAN integrity across a service-provider network. You configure a tunnel port on an edge switch in the service-provider network and connect it to an IEEE 802.1Q trunk port on a customer interface, creating an asymmetric link. A tunnel port belongs to a single VLAN that is dedicated to tunneling. For more information about tunnel ports, see Chapter 16, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”</td>
<td>VTP is not required. You manually assign the tunnel port to a VLAN by using the switchport access vlan interface configuration command.</td>
</tr>
</tbody>
</table>

For more detailed definitions of access and trunk modes and their functions, see Table 13-4 on page 13-17.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the “Managing the MAC Address Table” section on page 6-19.
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, use the commands described in these sections and in the command reference for this release. To change the VTP configuration, see Chapter 14, “Configuring VTP.”

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.

You can set these parameters when you create a new normal-range VLAN or modify an existing VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TrBRF, or TrCRF, Token Ring, Token Ring-Net)
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs
- VLAN number to use when translating from one VLAN type to another

This section does not provide configuration details for most of these parameters. For complete information on the commands and parameters that control VLAN configuration, see the command reference for this release.

These sections contain normal-range VLAN configuration information:

- **Token Ring VLANs**, page 13-6
- **Normal-Range VLAN Configuration Guidelines**, page 13-6
- **Configuring Normal-Range VLANs**, page 13-7
- **Default Ethernet VLAN Configuration**, page 13-7
- **Creating or Modifying an Ethernet VLAN**, page 13-8
- **Deleting a VLAN**, page 13-9
- **Assigning Static-Access Ports to a VLAN**, page 13-9
Token Ring VLANs

Although the switch does not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running VTP Version 2 advertise information about these Token Ring VLANs:

- Token Ring TrBRF VLANs
- Token Ring TrCRF VLANs

For more information on configuring Token Ring VLANs, see the Catalyst 5000 Series Software Configuration Guide.

Normal-Range VLAN Configuration Guidelines

Follow these guidelines when creating and modifying normal-range VLANs in your network:

- The switch supports 1005 VLANs in VTP client, server, and transparent modes.
- 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 configuration for VLANs 1 to 1005 are always saved in the VLAN database. If the VTP mode is transparent, VTP and VLAN configuration are also saved in the switch running configuration file.
- With VTP versions 1 and 2, the switch supports VLAN IDs 1006 through 4094 only in VTP transparent mode (VTP disabled). These are extended-range VLANs and configuration options are limited. Extended-range VLANs created in VTP transparent mode are not saved in the VLAN database and are not propagated. VTP version 3 supports extended range VLAN (VLANs 1006 to 4094) database propagation. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2. See the “Configuring Extended-Range VLANs” section on page 13-11.
- 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 128 spanning-tree instances. If a switch has more active VLANs than supported spanning-tree instances, spanning tree can be enabled on 128 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. For more information about MSTP, see Chapter 17, “Configuring MSTP.”
Configuring Normal-Range VLANs

You configure VLANs in `vlan` global configuration command by entering a VLAN ID. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN. You can use the default VLAN configuration (Table 13-2) or enter multiple commands to configure the VLAN. For more information about commands available in this mode, see the `vlan` global configuration command description in the command reference for this release. When you have finished the configuration, you must exit VLAN configuration mode for the configuration to take effect. To display the VLAN configuration, enter the `show vlan` privileged EXEC command.

The configurations of VLAN IDs 1 to 1005 are always saved in the VLAN database (vlan.dat file). If the VTP mode is transparent, they are also saved in the switch running configuration file. You can enter the `copy running-config startup-config` privileged EXEC command to save the configuration in the startup configuration file. To display the VLAN configuration, enter the `show vlan` 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 first 1005 VLANs use the VLAN database information.
- In VTP versions 1 and 2, if VTP mode is server, the domain name and VLAN configuration for only the first 1005 VLANs use the VLAN database information. VTP version 3 also supports VLANs 1006 to 4094.

Default Ethernet VLAN Configuration

Table 13-2 shows the default configuration for Ethernet VLANs.

The switch supports Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you only configure FDDI and Token Ring media-specific characteristics for VTP global advertisements to other switches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>1</td>
<td>1 to 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong>: Extended-range VLANs (VLAN IDs 1006 to 4094) are only saved in the VLAN database in VTP version 3.</td>
</tr>
<tr>
<td>VLAN name</td>
<td>VLANxxxx, where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number</td>
<td>No range</td>
</tr>
<tr>
<td>IEEE 802.10 SAID</td>
<td>100001 (100000 plus the VLAN ID)</td>
<td>1 to 4294967294</td>
</tr>
</tbody>
</table>
Configuring Normal-Range VLANs

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.

Note
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. See the “Configuring Extended-Range VLANs” section on page 13-11.

For the list of default parameters that are assigned when you add a VLAN, see the “Configuring Normal-Range VLANs” section on page 13-4.

Beginning in privileged EXEC mode, follow these steps to create or modify an Ethernet VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| 2      | vlan vlan-id    | Enter a VLAN ID, and enter 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.  
For information about adding VLAN IDs greater than 1005 (extended-range VLANs), see the “Configuring Extended-Range VLANs” section on page 13-11. |
| 3      | name vlan-name  | (Optional) Enter a name for the VLAN. If no name is entered for the VLAN, the default is to append the vlan-id with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4. |
| 4      | mtu mtu-size    | (Optional) Change the MTU size (or other VLAN characteristic).          |
| 5      | remote-span     | Note: (Optional) Configure the VLAN as the RSPAN VLAN for a remote SPAN session. For more information on remote SPAN, see Chapter 28, “Configuring SPAN and RSPAN.” |
| 6      | end             | Return to privileged EXEC mode.                                         |
Chapter 13  Configuring VLANs

Configuring Normal-Range VLANs

To return the VLAN name to the default settings, use the no name, no mtu, or no remote-span commands.

This example shows how to create Ethernet VLAN 20, name it test20, and add it to the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

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.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>no vlan vlan-id Remove the VLAN by entering the VLAN ID.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show vlan brief Verify the VLAN removal.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup config (Optional) If the switch is in VTP transparent mode, the VLAN configuration is saved in the running configuration file as well as in the VLAN database. This saves the configuration in the switch startup 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 are assigning a port on a cluster member switch to a VLAN, first use the rcommand privileged EXEC command to log in to the cluster member switch.
If you assign an interface to a VLAN that does not exist, the new VLAN is created. (See the “Creating or Modifying an Ethernet VLAN” section on page 13-8.)

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VLAN database:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode access</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport access vlan vlan-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config interface interface-id</td>
</tr>
<tr>
<td>Step 7</td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return an interface to its default configuration, use the **default interface interface-id** interface configuration command.

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 gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```
Configuring 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.

**Note**

Although the switch supports 4094 VLAN IDs, see the “Supported VLANs” section on page 13-2 for the actual number of VLANs supported.

These sections contain extended-range VLAN configuration information:

- Default VLAN Configuration, page 13-11
- Extended-Range VLAN Configuration Guidelines, page 13-11
- Creating an Extended-Range VLAN, page 13-12
- Creating an Extended-Range VLAN with an Internal VLAN ID, page 13-13

**Default VLAN Configuration**

See Table 13-2 on page 13-7 for the default configuration for Ethernet VLANs. You can change only the MTU size, private VLAN, and the remote SPAN configuration state on extended-range VLANs; all other characteristics must remain at the default state.

**Extended-Range VLAN Configuration Guidelines**

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.
- In VTP version 1 and 2, a switch must be in VTP transparent mode when you create extended-range VLANs. If VTP mode is server or client, an error message is generated, and the extended-range VLAN is rejected. VTP version 3 supports extended VLANs in server and transparent modes.
- For VTP version 1 or 2, you can set the VTP mode to transparent in global configuration mode. See the “Configuring VTP Mode” section on page 14-10. 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.
- STP is enabled by default on extended-range VLANs, but you can disable it by using the `no spanning-tree vlan vlan-id` global configuration command. When the maximum number of spanning-tree instances are on the switch, spanning tree is disabled on any newly created VLANs.
If the number of VLANs on the switch exceeds the maximum number of 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. For more information about MSTP, see Chapter 17, “Configuring MSTP.”

- Each routed port on the switch creates an internal VLAN for its use. These internal VLANs use extended-range VLAN numbers, and the internal VLAN ID cannot be used for an extended-range VLAN. If you try to create an extended-range VLAN with a VLAN ID that is already allocated as an internal VLAN, an error message is generated, and the command is rejected.
  - Because internal VLAN IDs are in the lower part of the extended range, we recommend that you create extended-range VLANs beginning from the highest number (4094) and moving to the lowest (1006) to reduce the possibility of using an internal VLAN ID.
  - Before configuring extended-range VLANs, enter the `show vlan internal usage` privileged EXEC command to see which VLANs have been allocated as internal VLANs.
  - If necessary, you can shut down the routed port assigned to the internal VLAN, which frees up the internal VLAN, and then create the extended-range VLAN and re-enable the port, which then uses another VLAN as its internal VLAN. See the “Creating an Extended-Range VLAN with an Internal VLAN ID” section on page 13-13.
- Although the switch supports a total of 1005 (normal-range and extended-range) VLANs, the number of routed ports, SVIs, and other configured features affects the use of the switch hardware. If you try to create an extended-range VLAN and there are not enough hardware resources available, an error message is generated, and the extended-range VLAN is rejected.

**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 (see Table 13-2) and the MTU size, private VLAN, and RSPAN configuration are the only parameters you can change. See the description of the `vlan` global configuration command in the command reference for the default settings of all parameters. In VTP version 1 or 2, if you enter an extended-range VLAN ID when the switch is not in VTP transparent mode, an error message is generated when you exit VLAN configuration mode, and the extended-range VLAN is not created.

In VTP version 1 and 2, extended-range VLANs are not saved in the VLAN database; they are saved in the switch running configuration file. You can save the extended-range VLAN configuration in the switch startup configuration file by using the `copy running-config startup-config` privileged EXEC command. VTP version 3 saves extended-range VLANs in the VLAN database.

**Note**

Before you create an extended-range VLAN, you can verify that the VLAN ID is not used internally by entering the `show vlan internal usage` privileged EXEC command. If the VLAN ID is used internally and you want to free it up, go to the “Creating an Extended-Range VLAN with an Internal VLAN ID” section on page 13-13 before creating the extended-range VLAN.
Beginning in privileged EXEC mode, follow these steps to create an extended-range VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>vtp mode transparent</td>
<td>Configure the switch for VTP transparent mode, disabling VTP.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This step is not required for VTP version 3.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>Enter an extended-range VLAN ID and enter VLAN configuration mode. The range is 1006 to 4094.</td>
</tr>
<tr>
<td>mtu mtu-size</td>
<td>(Optional) Modify the VLAN by changing the MTU size.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Although all VLAN commands appear in the CLI help, only the mtu mtu-size, private-vlan, and remote-span commands are supported for extended-range VLANs.</td>
</tr>
<tr>
<td>remote-span</td>
<td>(Optional) Configure the VLAN as the RSPAN VLAN. See the “Configuring a VLAN as an RSPAN VLAN” section on page 28-17.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show vlan id vlan-id</td>
<td>Verify that the VLAN has been created.</td>
</tr>
<tr>
<td>copy running-config startup config</td>
<td>Save your entries in the switch startup configuration file. To save extended-range VLAN configurations, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> With VTP version 3, the VLAN configuration is also saved in the VLAN database.</td>
</tr>
</tbody>
</table>

To delete an extended-range VLAN, use the no vlan vlan-id global configuration command.

The procedure for assigning static-access ports to an extended-range VLAN is the same as for normal-range VLANs. See the “Assigning Static-Access Ports to a VLAN” section on page 13-9.

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
```

**Creating an Extended-Range VLAN with an Internal VLAN ID**

If you enter an extended-range VLAN ID that is already assigned to an internal VLAN, an error message is generated, and the extended-range VLAN is rejected. To manually free an internal VLAN ID, you must temporarily shut down the routed port that is using the internal VLAN ID.
Beginning in privileged EXEC mode, follow these steps to release a VLAN ID that is assigned to an internal VLAN and to create an extended-range VLAN with that ID:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 show vlan internal usage</td>
<td>Display the VLAN IDs being used internally by the switch. If the VLAN ID that you want to use is an internal VLAN, the display shows the routed port that is using the VLAN ID. Enter that port number in Step 3.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Specify the interface ID for the routed port that is using the VLAN ID, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 shutdown</td>
<td>Shut down the port to free the internal VLAN ID.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6 vtp mode transparent</td>
<td>Set the VTP mode to transparent for creating extended-range VLANs.</td>
</tr>
<tr>
<td>Step 7 vlan vlan-id</td>
<td>Enter the new extended-range VLAN ID, and enter VLAN configuration mode.</td>
</tr>
<tr>
<td>Step 8 exit</td>
<td>Exit from VLAN configuration mode, and return to global configuration mode.</td>
</tr>
<tr>
<td>Step 9 interface interface-id</td>
<td>Specify the interface ID for the routed port that you shut down in Step 4, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 10 no shutdown</td>
<td>Re-enable the routed port. It will be assigned a new internal VLAN ID.</td>
</tr>
<tr>
<td>Step 11 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 12 copy running-config startup config</td>
<td>Save your entries in the switch startup configuration file. To save an extended-range VLAN configuration, you need to save the VTP transparent mode configuration and the extended-range VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it will default to VTP server mode, and the extended-range VLAN IDs will not be saved.</td>
</tr>
</tbody>
</table>

Note: This step is not required for VTP version 3 because VLANs are saved in the VLAN database.
Displaying VLANs

Use the `show vlan` privileged EXEC command to display a list of all VLANs on the switch, including extended-range VLANs. The display includes VLAN status, ports, and configuration information.

Table 13-3 lists the privileged EXEC commands for monitoring VLANs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces</code></td>
<td>Display characteristics for all interfaces or for the specified VLAN configured on the switch.</td>
</tr>
<tr>
<td><code>vlan vlan-id</code></td>
<td></td>
</tr>
<tr>
<td><code>show vlan</code></td>
<td>Display parameters for all VLANs or the specified VLAN on the switch.</td>
</tr>
<tr>
<td><code>id vlan-id</code></td>
<td></td>
</tr>
</tbody>
</table>

For more details about the `show` command options and explanations of output fields, see the command reference for this release.
Configuring VLAN Trunks

These sections contain this conceptual information:

- Trunking Overview, page 13-16
- Encapsulation Types, page 13-18
- Default Layer 2 Ethernet Interface VLAN Configuration, page 13-19
- Configuring an Ethernet Interface as a Trunk Port, page 13-19
- Configuring Trunk Ports for Load Sharing, page 13-24

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.

Two trunking encapsulations are available on all Ethernet interfaces:

- Inter-Switch Link (ISL) — Cisco-proprietary trunking encapsulation.
- IEEE 802.1Q — industry-standard trunking encapsulation.

Figure 13-2 shows a network of switches that are connected by ISL trunks.

![Figure 13-2 Switches in an ISL Trunking Environment](image)

You can configure a trunk on a single Ethernet interface or on an EtherChannel bundle. For more information about EtherChannel, see Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

Ethernet trunk interfaces support different trunking modes (see Table 13-4). 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. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations.

To avoid this, you should 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. Use the `switchport trunk encapsulation isl` or `switchport trunk encapsulation dot1q` interface to select the encapsulation type on the trunk port.

You can also specify on DTP interfaces whether the trunk uses ISL or IEEE 802.1Q encapsulation or if the encapsulation type is autonegotiated. The DTP supports autonegotiation of both ISL and IEEE 802.1Q trunks.

<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>
<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 <code>trunk</code> or <code>desirable</code> mode. The default switchport mode for all Ethernet interfaces is <code>dynamic auto</code>.</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 <code>trunk</code>, <code>desirable</code>, or <code>auto</code> 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 <code>access</code> or <code>trunk</code>. You must manually configure the neighboring interface as a trunk interface to establish a trunk link.</td>
</tr>
<tr>
<td>switchport mode dot1q-tunnel</td>
<td>Configures the interface as a tunnel (nontrunking) port to be connected in an asymmetric link with an IEEE 802.1Q trunk port. The IEEE 802.1Q tunneling is used to maintain customer VLAN integrity across a service provider network. See Chapter 16, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling,” for more information on tunnel ports.</td>
</tr>
</tbody>
</table>

---

DTP is not supported on private-VLAN ports or tunnel ports.
Encapsulation Types

Table 13-5 lists the Ethernet trunk encapsulation types and keywords.

Table 13-5  Ethernet Trunk Encapsulation Types

<table>
<thead>
<tr>
<th>Encapsulation</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport trunk encapsulation isl</td>
<td>Specifies ISL encapsulation on the trunk link.</td>
</tr>
<tr>
<td>switchport trunk encapsulation dot1q</td>
<td>Specifies IEEE 802.1Q encapsulation on the trunk link.</td>
</tr>
<tr>
<td>switchport trunk encapsulation negotiate</td>
<td>Specifies that the interface negotiate with the neighboring interface to become an ISL (preferred) or IEEE 802.1Q trunk, depending on the configuration and capabilities of the neighboring interface. This is the default for the switch.</td>
</tr>
</tbody>
</table>

Note: The switch does not support Layer 3 trunks. You cannot configure subinterfaces or use the encapsulation keyword on Layer 3 interfaces. The switch does support Layer 2 trunks and Layer 3 VLAN interfaces, which provide equivalent capabilities.

IEEE 802.1Q Configuration Considerations

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 you disable spanning tree.
Default Layer 2 Ethernet Interface VLAN Configuration

Table 13-6 shows the 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>Trunk encapsulation</td>
<td>switchport trunk encapsulation negotiate</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>

Configuring an Ethernet Interface as 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.

These sections contain this configuration information:

- Interaction with Other Features, page 13-19
- Defining the Allowed VLANs on a Trunk, page 13-22
- Changing the Pruning-Eligible List, page 13-23
- Configuring the Native VLAN for Untagged Traffic, page 13-24

Note

By default, an interface is in Layer 2 mode. The default mode for Layer 2 interfaces is switchport mode dynamic auto. If the neighboring interface supports trunking and is configured to allow trunking, the link is a Layer 2 trunk or, if the interface is in Layer 3 mode, it becomes a Layer 2 trunk when you enter the switchport interface configuration command. By default, trunks negotiate encapsulation. If the neighboring interface supports ISL and IEEE 802.1Q encapsulation and both interfaces are set to negotiate the encapsulation type, the trunk uses ISL encapsulation.

Interaction with Other Features

Trunking interacts with other features in these ways:

- A trunk port cannot be a secure port.
- A trunk port cannot be a tunnel 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 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 PVST mode and no more than 40 trunk ports in 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.
### Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a port as a trunk port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</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>2</td>
<td><code>interface interface-id</code></td>
<td>Specify the port to be configured for trunking, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>`switchport trunk encapsulation {isl</td>
<td>dot1q</td>
</tr>
<tr>
<td>4</td>
<td>`switchport mode {dynamic {auto</td>
<td>desirable}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dynamic auto</code>—Set the interface to a trunk link if the neighboring interface is set to trunk or desirable mode. This is the default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>dynamic desirable</code>—Set the interface to a trunk link if the neighboring interface is set to trunk, desirable, or auto mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>trunk</code>—Set 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>5</td>
<td><code>switchport access vlan vlan-id</code></td>
<td>(Optional) Specify the default VLAN, which is used if the interface stops trunking.</td>
</tr>
<tr>
<td>6</td>
<td><code>switchport trunk native vlan vlan-id</code></td>
<td>Specify the native VLAN for IEEE 802.1Q trunks.</td>
</tr>
<tr>
<td>7</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td><code>show interfaces interface-id switchport</code></td>
<td>Display the switchport configuration of the interface in the Administrative Mode and the Administrative Trunking Encapsulation fields of the display.</td>
</tr>
<tr>
<td>9</td>
<td><code>show interfaces interface-id trunk</code></td>
<td>Display the trunk configuration of the interface.</td>
</tr>
<tr>
<td>10</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return an interface to its default configuration, use the `default interface interface-id` interface configuration command. To reset all trunking characteristics of a trunking interface to the defaults, use the `no switchport trunk` interface configuration command. To disable trunking, use the `switchport mode access` interface configuration command to configure the port as a static-access port.

This 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)# interface gigabitethernet0/2
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# end
```
Defining the 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 restrict the traffic a trunk carries, use the `switchport trunk allowed vlan remove vlan-list` interface configuration command to remove specific VLANs from the allowed list.

**Note**

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.

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.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of a trunk:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Specify the port to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td></td>
<td>Configure the interface as a VLAN trunk port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport trunk allowed vlan [add</td>
</tr>
<tr>
<td></td>
<td>(Optional) Configure the list of VLANs allowed on the trunk.</td>
</tr>
<tr>
<td></td>
<td>For explanations about using the add, all, except, and remove keywords, see the command reference for this release.</td>
</tr>
<tr>
<td></td>
<td>The vlan-list parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated VLAN parameters or in hyphen-specified ranges.</td>
</tr>
<tr>
<td></td>
<td>All VLANs are allowed by default.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td></td>
<td>Verify your entries in the Trunking VLANs Enabled field of the display.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To return to the default allowed VLAN list of all VLANs, use the `no switchport trunk allowed vlan` interface configuration command.

This example shows how to remove VLAN 2 from the allowed VLAN list on a port:

```bash
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

### 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. The “Enabling VTP Pruning” section on page 14-14 describes how to enable VTP pruning.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`switchport trunk pruning vlan {add</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show interfaces interface-id switchport</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

To return to the default pruning-eligible list of all VLANs, use the `no switchport trunk pruning vlan` interface configuration command.
## 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.

- **Note**: The native VLAN can be assigned any VLAN ID.

For information about IEEE 802.1Q configuration issues, see the “IEEE 802.1Q Configuration Considerations” section on page 13-18.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an IEEE 802.1Q trunk:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport trunk native vlan vlan-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default native VLAN, VLAN 1, use the no switchport trunk native vlan interface configuration command.

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.

## Configuring Trunk Ports for Load Sharing

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. For more information about STP, see Chapter 26, “Configuring STP.”
Load Sharing Using STP Port 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.

Figure 13-3 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 16 on Trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on Trunk 1.
- VLANs 3 through 6 are assigned a port priority of 16 on Trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on Trunk 2.

In this way, Trunk 1 carries traffic for VLANs 8 through 10, and Trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

Figure 13-3  Load Sharing by Using STP Port Priorities

Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 13-3.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode on Switch A.</td>
</tr>
<tr>
<td>Step 2 vtp domain domain-name</td>
<td>Configure a VTP administrative domain. The domain name can be 1 to 32 characters.</td>
</tr>
<tr>
<td>Step 3 vtp mode server</td>
<td>Configure Switch A as the VTP server.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show vtp status</td>
<td>Verify the VTP configuration on both Switch A and Switch B. In the display, check the VTP Operating Mode and the VTP Domain Name fields.</td>
</tr>
<tr>
<td>Step 6 show vlan</td>
<td>Verify that the VLANs exist in the database on Switch A.</td>
</tr>
<tr>
<td>Step 7 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 8 interface interface-id_1</td>
<td>Define the interface to be configured as a trunk, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
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.

In Figure 13-4, Trunk ports 1 and 2 are configured as 100BASE-T ports. These VLAN path costs are assigned:

- VLANs 2 through 4 are assigned a path cost of 30 on Trunk port 1.
- VLANs 8 through 10 retain the default 100BASE-T path cost on Trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on Trunk port 2.
- VLANs 2 through 4 retain the default 100BASE-T path cost on Trunk port 2 of 19.
Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 13-4:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode on Switch A.</td>
</tr>
<tr>
<td>Step 2 interface interface-id_1</td>
<td>Define the interface to be configured as a trunk, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 switchport trunk encapsulation {isl</td>
<td>dot1q</td>
</tr>
<tr>
<td>Step 4 switchport mode trunk</td>
<td>Configure the port as a trunk port. The trunk defaults to ISL trunking.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Repeat Steps 2 through 5 on a second interface in Switch A.</td>
</tr>
<tr>
<td>Step 7 show running-config</td>
<td>Verify your entries. In the display, make sure that the interfaces are configured as trunk ports.</td>
</tr>
<tr>
<td>Step 8 show vlan</td>
<td>When the trunk links come up, Switch A receives the VTP information from the other switches. Verify that Switch A has learned the VLAN configuration.</td>
</tr>
<tr>
<td>Step 9 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 10 interface interface-id_1</td>
<td>Define the interface on which to set the STP cost, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 11 spanning-tree vlan 2-4 cost 30</td>
<td>Set the spanning-tree path cost to 30 for VLANs 2 through 4.</td>
</tr>
<tr>
<td>Step 12 end</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 13 exit</td>
<td>Repeat Steps 9 through 13 on the other configured trunk interface on Switch A, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.</td>
</tr>
<tr>
<td>Step 14 exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 15 show running-config</td>
<td>Verify your entries. In the display, verify that the path costs are set correctly for both trunk interfaces.</td>
</tr>
<tr>
<td>Step 16 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Configuring VMPS

The VLAN Query Protocol (VQP) is used to support dynamic-access ports, which are not permanently assigned to a VLAN, but give VLAN assignments based on the MAC source addresses seen on the port. Each time an unknown MAC address is seen, the switch sends a VQP query to a remote VMPS; the query includes the newly seen MAC address and the port on which it was seen. The VMPS responds with a VLAN assignment for the port. The switch cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

These sections contain this information:

- “Understanding VMPS” section on page 13-28
- “Default VMPS Client Configuration” section on page 13-29
- “VMPS Configuration Guidelines” section on page 13-29
- “Configuring the VMPS Client” section on page 13-30
- “Monitoring the VMPS” section on page 13-33
- “Troubleshooting Dynamic-Access Port VLAN Membership” section on page 13-33
- “VMPS Configuration Example” section on page 13-33

Understanding VMPS

Each time the client switch receives the MAC address of a new host, it sends a VQP query to the VMPS. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in open or secure mode. In secure mode, the server shuts down the port when an illegal host is detected. In open mode, the server simply denies the host access to the port.

If the port is currently unassigned (that is, it does not yet have a VLAN assignment), the VMPS provides one of these responses:

- If the host is allowed on the port, the VMPS sends the client a vlan-assignment response containing the assigned VLAN name and allowing access to the host.
- If the host is not allowed on the port and the VMPS is in open mode, the VMPS sends an access-denied response.
- If the VLAN is not allowed on the port and the VMPS is in secure mode, the VMPS sends a port-shutdown response.

If the port already has a VLAN assignment, the VMPS provides one of these responses:

- If the VLAN in the database matches the current VLAN on the port, the VMPS sends an success response, allowing access to the host.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an access-denied or a port-shutdown response, depending on the secure mode of the VMPS.

If the switch receives an access-denied response from the VMPS, it continues to block traffic to and from the host MAC address. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new host address. If the switch receives a port-shutdown response from the VMPS, it disables the port. The port must be manually re-enabled by using Network Assistant, the CLI, or SNMP.
Dynamic-Access Port VLAN Membership

A dynamic-access port can belong to only one VLAN with an ID from 1 to 4094. When the link comes up, the switch does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic-access port and attempts to match the MAC address to a VLAN in the VMPS database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

Multiple hosts (MAC addresses) can be active on a dynamic-access port if they are all in the same VLAN; however, the VMPS shuts down a dynamic-access port if more than 20 hosts are active on the port.

If the link goes down on a dynamic-access port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again through the VQP with the VMPS before the port is assigned to a VLAN.

Dynamic-access ports can be used for direct host connections, or they can connect to a network. A maximum of 20 MAC addresses are allowed per port on the switch. A dynamic-access port can belong to only one VLAN at a time, but the VLAN can change over time, depending on the MAC addresses seen.

Default VMPS Client Configuration

Table 13-7 shows the default VMPS and dynamic-access port configuration on client switches.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMPS domain server</td>
<td>None</td>
</tr>
<tr>
<td>VMPS reconfirm interval</td>
<td>60 minutes</td>
</tr>
<tr>
<td>VMPS server retry count</td>
<td>3</td>
</tr>
<tr>
<td>Dynamic-access ports</td>
<td>None configured</td>
</tr>
</tbody>
</table>

VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic-access port VLAN membership:

- You should configure the VMPS before you configure ports as dynamic-access ports.
- When you configure a port as a dynamic-access port, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state.
- IEEE 802.1x ports cannot be configured as dynamic-access ports. If you try to enable IEEE 802.1x on a dynamic-access (VQP) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
Trunk ports cannot be dynamic-access ports, but you can enter the `switchport access vlan dynamic` interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

You must turn off trunking on the port before the dynamic-access setting takes effect.

Dynamic-access ports cannot be monitor ports.

Secure ports cannot be dynamic-access ports. You must disable port security on a port before it becomes dynamic.

Private VLAN ports cannot be dynamic-access ports.

Dynamic-access ports cannot be members of an EtherChannel group.

Port channels cannot be configured as dynamic-access ports.

A dynamic-access port can participate in fallback bridging.

The VTP management domain of the VMPS client and the VMPS server must be the same.

The VLAN configured on the VMPS server should not be a voice VLAN.

### Configuring the VMPS Client

You configure dynamic VLANs by using the VMPS (server). The switch can be a VMPS client; it cannot be a VMPS server.

### Entering the IP Address of the VMPS

You must first enter the IP address of the server to configure the switch as a client.

Note: If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: vmps server ipaddress primary</td>
<td>Enter the IP address of the switch acting as the primary VMPS server.</td>
</tr>
<tr>
<td>Step 3: vmps server ipaddress</td>
<td>(Optional) Enter the IP address of the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5: show vmps</td>
<td>Verify your entries in the VMPS Domain Server field of the display.</td>
</tr>
<tr>
<td>Step 6: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Note: You must have IP connectivity to the VMPS for dynamic-access ports to work. You can test for IP connectivity by pinging the IP address of the VMPS and verifying that you get a response.
## Configuring Dynamic-Access Ports on VMPS Clients

If you are configuring a port on a cluster member switch as a dynamic-access port, first use the `rcommand` privileged EXEC command to log in to the cluster member switch.

**Caution**

Dynamic-access port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic-access ports to other switches can cause a loss of connectivity.

Beginning in privileged EXEC mode, follow these steps to configure a dynamic-access port on a VMPS client switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode access</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport access vlan dynamic</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show interfaces interface-id switchport</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return an interface to its default configuration, use the `default interface interface-id` interface configuration command. To return an interface to its default switchport mode (dynamic auto), use the `no switchport mode` interface configuration command. To reset the access mode to the default VLAN for the switch, use the `no switchport access vlan` interface configuration command.

## Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic-access port VLAN membership assignments that the switch has received from the VMPS:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>vmps reconfirm</td>
</tr>
<tr>
<td>Step 2</td>
<td>show vmps</td>
</tr>
</tbody>
</table>
Chapter 13  Configuring VLANs

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs.

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command switch. You must also first use the `rcommand` privileged EXEC command to log in to the member switch.

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>vmps reconfirm minutes</code> Enter the number of minutes between reconfirmations of the dynamic VLAN membership. The range is 1 to 120. The default is 60 minutes.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show vmps</code> Verify the dynamic VLAN reconfirmation status in the <code>Reconfirm Interval</code> field of the display.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no vmps reconfirm` global configuration command.

Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch attempts to contact the VMPS before querying the next server:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>vmps retry count</code> Change the retry count. The retry range is 1 to 10; the default is 3.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show vmps</code> Verify your entry in the <code>Server Retry Count</code> field of the display.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no vmps retry` global configuration command.
Monitoring the VMPS

You can display information about the VMPS by using the `show vmps` privileged EXEC command. The switch displays this information about the VMPS:

- **VMPS VQP Version**—the version of VQP used to communicate with the VMPS. The switch queries the VMPS that is using VQP Version 1.
- **Reconfirm Interval**—the number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.
- **Server Retry Count**—the number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.
- **VMPS domain server**—the IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked `current`. The one marked `primary` is the primary server.
- **VMPS Action**—the result of the most recent reconfirmation attempt. A reconfirmation attempt can occur automatically when the reconfirmation interval expires, or you can force it by entering the `vmps reconfirm` privileged EXEC command or its Network Assistant or SNMP equivalent.

This is an example of output for the `show vmps` privileged EXEC command:

```
Switch# show vmps
VQP Client Status:
-------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         other
```

Troubleshooting Dynamic-Access Port VLAN Membership

The VMPS shuts down a dynamic-access port under these conditions:

- The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic-access port.

To re-enable a disabled dynamic-access port, enter the `shutdown` interface configuration command followed by the `no shutdown` interface configuration command.

VMPS Configuration Example

**Figure 13-5** shows a network with a VMPS server switch and VMPS client switches with dynamic-access ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 6500 series Switch A is the primary VMPS server.
- The Catalyst 6500 series Switch C and Switch J are secondary VMPS servers.
- End stations are connected to the clients, Switch B and Switch I.
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.

Figure 13-5  Dynamic Port VLAN Membership Configuration

![Diagram showing VLAN configuration with end stations, switches, and TFTP server.](image-url)
CHAPTER 14

Configuring VTP

This chapter describes how to use the VLAN Trunking Protocol (VTP) and the VLAN database for managing VLANs with the Catalyst 3560 switches. For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter consists of these sections:

- Understanding VTP, page 14-1
- Configuring VTP, page 14-7
- Monitoring VTP, page 14-16

Understanding 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.

Before you create VLANs, you must decide whether to use 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 1005 VLANs, but the number of routed ports, SVIs, and other configured features affects the usage of the switch hardware. 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.

VTP version 1 and version 2 support only normal-range VLANs (VLAN IDs 1 to 1005). 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.
These sections contain this conceptual information:

- The VTP Domain, page 14-2
- VTP Modes, page 14-3
- VTP Advertisements, page 14-3
- VTP Version 2, page 14-4
- VTP Version 3, page 14-5
- VTP Pruning, page 14-5

### The 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.

Caution

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. See the “Adding a VTP Client Switch to a VTP Domain” section on page 14-15 for the procedure for verifying and resetting the VTP 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 Inter-Switch Link (ISL) and 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.

For domain name and password configuration guidelines, see the “VTP Configuration Guidelines” section on page 14-8.
VTP Modes

You can configure a supported switch to be in one of the VTP modes listed in Table 14-1.

Table 14-1 VTP Modes

<table>
<thead>
<tr>
<th>VTP Mode</th>
<th>Description</th>
</tr>
</thead>
</table>
| VTP server   | 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.  

*Note* 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. |
| VTP client   | A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. 

In VTP versions 1 and 2, in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode. |
| VTP transparent | VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. 

In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create extended-range VLANs. VTP version 3 also supports creating extended-range VLANs in client or server mode. See the “Configuring Extended-Range VLANs” section on page 13-11. 

In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create private VLANs and when they are configured, you should not change the VTP mode from transparent to client or server mode. VTP version 3 also supports private VLANs in client and server modes. See Chapter 15, “Configuring Private VLANs.” 

When the switch is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other switches. In this mode, VTP mode and domain name are saved in the switch running configuration, and you can save this information in the switch startup configuration file by using the `copy running-config startup-config` privileged EXEC command. |
| VTP off      | A switch in VTP off mode functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks. |

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.
Understanding VTP

Note
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. For more information on trunk ports, see the “Configuring VLAN Trunks” section on page 13-16.

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 (ISL and 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.

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. For more information about Token Ring VLANs, see the “Configuring Normal-Range VLANs” section on page 13-4.
- 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. Because VTP version 2 supports only one domain, it forwards VTP messages in transparent mode without inspecting the version and domain name.
- 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.
Chapter 14 Configuring VTP

Understanding VTP

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. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2.

Note  VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

- Private VLAN support.

- 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.

- The option to turn VTP on or off on a per-trunk (per-port) basis. You can enable or disable VTP per port by entering the [no] vtp interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot set VTP to off for the MST database and on for the VLAN database on the same port.

When you globally set VTP mode to off, it applies to all the trunking ports in the system. However, you can specify on or off on a per-VTP instance basis. For example, you can configure the switch as a VTP server for the VLAN database but with VTP off for the MST database.

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.
Figure 14-1 shows a switched network without VTP pruning enabled. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.

Figure 14-1 Flooding Traffic without VTP Pruning

Enabling VTP pruning on a VTP server enables pruning for the entire management 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).
See the “Enabling VTP Pruning” section on page 14-14. 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 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:

- 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 (see the “Changing the Pruning-Eligible List” section on page 13-23). 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.

### Configuring VTP

These sections contain this configuration information:

- Default VTP Configuration, page 14-7
- VTP Configuration Guidelines, page 14-8
- Configuring VTP Mode, page 14-10
- Enabling the VTP Version, page 14-13
- Enabling VTP Pruning, page 14-14
- Configuring VTP on a Per-Port Basis, page 14-15
- Adding a VTP Client Switch to a VTP Domain, page 14-15

### Default VTP Configuration

Table 14-2 shows the 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>
VTP Configuration Guidelines

You use the `vtp` global configuration command to set the VTP password, the version, the VTP file name, the interface providing updated VTP information, the domain name, and the mode, and to disable or enable pruning. For more information about available keywords, see the command descriptions in the command reference for this release. 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 if the switch resets.

When you save VTP information in the switch startup configuration file and restart the switch, the configuration is selected as follows:

- If the VTP mode is transparent in both 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). 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 the domain name in the startup configuration do not match the VLAN database, the domain name and the VTP mode and configuration for the first 1005 VLANs use the VLAN database information.

Domain Names

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 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

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.

### 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.
- We recommend 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. You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured.
- 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.
Configuring 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.

For more information, see the “Configuring VLAN Trunks” section on page 13-16.

If you are configuring VTP on a cluster member switch to a VLAN, use the rcommand privileged EXEC command to log in to the member switch. For more information about the command, see the command reference for this release.

In VTP versions 1 and 2, when you configure extended-range VLANs on the switch, the switch must be in VTP transparent mode. VTP version 3 also supports creating extended-range VLANs in client or server mode.

VTP versions 1 and 2 do not support private VLANs. If you configure private VLANs, the switch must be in VTP transparent mode. When private VLANs are configured on the switch, do not change the VTP mode from transparent to client or server mode. VTP version 3 does support private VLANs.

Configuring VTP Mode

You can configure VTP mode as one of these:

- When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.
- When a switch is 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.
- When you configure the switch for 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 switches. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements on its trunk links.
- **VTP off mode** is the same as VTP transparent mode except that VTP advertisements are not forwarded.

Follow these guidelines:

- For VTP version 1 and version 2, if extended-range VLANs are configured on the switch, you cannot change VTP mode to client or server. You receive an error message, and the configuration is not allowed. 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.

**Note**

For VTP version 1 and 2, before you create extended-range VLANs (VLAN IDs 1006 to 4094), you must set VTP mode to transparent by using the vtp mode transparent global configuration command. Save this configuration to the startup configuration so that the switch starts in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets and boots up in VTP server mode (the default).

- VTP version 3 supports extended-range VLANs. If extended VLANs are configured, you cannot convert from VTP version 3 to VTP version 2.
Chapter 14 Configuring VTP

Configuring VTP

If you configure the switch for VTP client mode, the switch does not create the VLAN database file (vlan.dat). If the switch is then powered off, it resets the VTP configuration to the default. To keep the VTP configuration with VTP client mode after the switch restarts, you must first configure the VTP domain name before the VTP mode.

Caution

If all switches are operating in VTP client mode, do not configure a VTP domain name. If you do, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch as a VTP server.

Beginning in privileged EXEC mode, follow these steps to configure the VTP mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>vtp domain domain-name</td>
</tr>
<tr>
<td>Step 3</td>
<td>vtp mode {client</td>
</tr>
<tr>
<td>Step 4</td>
<td>vtp password password</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show vtp status</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.
To return a switch in another mode to VTP server mode, use the `no vtp mode` global configuration command. To return the switch to a no-password state, use the `no vtp password` global configuration command.

This example shows how to configure the switch as a VTP server with the domain name `eng_group` and the password `mypassword`:

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

### Configuring a VTP Version 3 Password

Beginning in privileged EXEC mode, follow these steps to configure the password when using VTP version 3:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>vtp password password [hidden</td>
</tr>
<tr>
<td></td>
<td>(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) hidden—Enter hidden to ensure that the secret key generated from the password string is saved 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) secret—Enter secret to directly configure the password. The secret password must contain 32 hexadecimal characters.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show vtp password</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save the configuration in the startup configuration file.</td>
</tr>
</tbody>
</table>

To clear the password, enter the `no vtp password` global configuration command.

This example shows how to configure a hidden password and how it appears.

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```
Configuring a VTP Version 3 Primary Server

Beginning in privileged EXEC mode, follow these steps on a VTP server to configure it as a VTP primary server (version 3 only), which starts a takeover operation:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 vtp primary-server [vlan</td>
<td>Change the operational state of a switch from a secondary server (the</td>
</tr>
<tr>
<td>mst]  [force]</td>
<td>default) to a primary server and advertise the configuration to the domain.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) vlan—Select the VLAN database as the takeover feature.</td>
</tr>
<tr>
<td></td>
<td>This is the default.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) mst—Select the multiple spanning tree (MST) database as</td>
</tr>
<tr>
<td></td>
<td>the takeover feature.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) force—Entering force overwrites the configuration of any</td>
</tr>
<tr>
<td></td>
<td>conflicting servers. If you do not enter force, you are prompted for</td>
</tr>
<tr>
<td></td>
<td>confirmation before the takeover.</td>
</tr>
</tbody>
</table>

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
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP domain

VTP Database Conf Switch ID  Primary Server Revision System Name
------------------------- ------ ---------------------------- -------------- ---------------
VLANDB        Yes 00d0.00b8.1400=00d0.00b8.1400   1       stp7

Do you want to continue (y/n) [n]? y
```

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, no private 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 must be disabled.
- VTP version 3 is supported on switches running Cisco IOS Release 12.2(52) SE or later.
Configuring VTP

Caution

In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

For more information on VTP version configuration guidelines, see the “VTP Version” section on page 14-9.

Beginning in privileged EXEC mode, follow these steps to configure the VTP version:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>vtp version {1 2 3}</td>
<td>Enable the VTP version on the switch. The default is VTP version 1.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show vtp status</td>
<td>Verify that the configured VTP version is enabled.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save the configuration in the startup configuration file.</td>
</tr>
</tbody>
</table>

To return to the default VTP version 1, use the **no vtp version** global configuration command.

Enabling VTP Pruning

Pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the destination devices. You can only enable VTP pruning on a switch in VTP server mode.

Beginning in privileged EXEC mode, follow these steps to enable VTP pruning in the VTP domain:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>vtp pruning</td>
<td>Enable pruning in the VTP administrative domain. By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show vtp status</td>
<td>Verify your entries in the <em>VTP Pruning Mode</em> field of the display.</td>
</tr>
</tbody>
</table>

To disable VTP pruning, use the **no vtp pruning** global configuration command.

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.

Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning-eligible on trunk ports. Reserved VLANs and extended-range VLANs cannot be pruned. To change the pruning-eligible VLANs, see the “Changing the Pruning-Eligible List” section on page 13-23.
Chapter 14  Configuring VTP

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.

Beginning in privileged EXEC mode, follow these steps to enable VTP on a port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Identify an interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 vtp</td>
<td>Enable VTP on the specified port.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config interface interface-id</td>
<td>Verify the change to the port.</td>
</tr>
<tr>
<td>Step 6 show vtp status</td>
<td>Verify the configuration.</td>
</tr>
</tbody>
</table>

To disable VTP on the interface, use the no vtp interface configuration command.

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# vtp
Switch(config-if)# end
```

Adding a VTP Client Switch to a VTP Domain

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.

Beginning in privileged EXEC mode, follow these steps to verify and reset the VTP configuration revision number on a switch before adding it to a VTP domain:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 show vtp status</td>
<td>Check the VTP configuration revision number.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 3 vtp domain domain-name</td>
<td>Change the domain name from the original one displayed in Step 1 to a new name.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>The VLAN information on the switch is updated and the configuration revision number is reset to 0. You return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 14 Configuring VTP

Monitoring VTP

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 14-3 shows the privileged EXEC commands for monitoring VTP activity.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vtp counters</td>
<td>Display counters about VTP messages that have been sent and received.</td>
</tr>
<tr>
<td>show vtp devices [conflict]</td>
<td>Display information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The show vtp devices 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>Display VTP status and configuration for all interfaces or the specified interface.</td>
</tr>
<tr>
<td>show vtp password</td>
<td>Display the VTP password. The form of the password displayed depends on whether or not the hidden keyword was entered and if encryption is enabled on the switch.</td>
</tr>
<tr>
<td>show vtp status</td>
<td>Display the VTP switch configuration information.</td>
</tr>
</tbody>
</table>

After resetting the configuration revision number, add the switch to the VTP domain.

Note

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.
Configuring Voice VLAN

This chapter describes how to configure the voice VLAN feature on the Catalyst 3560 switch. Voice VLAN is referred to as an auxiliary VLAN in some Catalyst 6500 family switch documentation.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding Voice VLAN, page 12-1
- Configuring Voice VLAN, page 12-3
- Displaying Voice VLAN, page 12-8

Understanding Voice VLAN

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. When the switch is connected to a Cisco 7960 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. For more information on QoS, see Chapter 34, “Configuring QoS.”

The Cisco 7960 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.

The Cisco IP Phone contains an integrated three-port 10/100 switch as shown in Figure 12-1. The ports provide dedicated connections to these devices:

- Port 1 connects to the switch or other voice-over-IP (VoIP) device.
- Port 2 is an internal 10/100 interface that carries the IP Phone traffic.
- Port 3 (access port) connects to a PC or other device.
Figure 12-1 shows one way to connect a Cisco 7960 IP Phone.

**Figure 12-1 Cisco 7960 IP Phone Connected to a Switch**

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).
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 (see Figure 12-1). 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.

Configuring Voice VLAN

These sections contain this configuration information:
- Default Voice VLAN Configuration, page 12-3
- Voice VLAN Configuration Guidelines, page 12-3
- Configuring a Port Connected to a Cisco 7960 IP Phone, page 12-5

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.

Voice VLAN Configuration Guidelines

These are the voice VLAN configuration guidelines:
- Voice VLAN configuration is only supported on switch access ports; voice VLAN configuration is not supported on trunk ports. You can configure a voice VLAN only on Layer 2 ports.

Note
Trunk ports can carry any number of voice VLANs, similar to regular VLANs. The configuration of voice VLANs is not required on trunk ports.

- 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, see Chapter 13, “Configuring VLANs,” for information on how to create the voice VLAN.
• Do not configure voice VLAN on private VLAN ports.
• 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. For information about PoE interfaces, see the “Configuring a Power Management Mode on a PoE Port” section on page 11-22.
• 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. If you use the auto-QoS feature, these settings are automatically configured. For more information, see Chapter 34, “Configuring QoS.”
• 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.)
• 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).
• You cannot configure static secure MAC addresses in the voice VLAN.
• Voice VLAN ports can also be these port types:
  – Dynamic access port. See the “Configuring Dynamic-Access Ports on VMPS Clients” section on page 13-31 for more information.
  – IEEE 802.1x authenticated port. See the “Configuring 802.1x Readiness Check” section on page 10-37 for more information.

| Note | 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. See the “Configuring Protected Ports” section on page 23-6 for more information.
  – A source or destination port for a SPAN or RSPAN session.
  – Secure port. See the “Configuring Port Security” section on page 23-9 for more information.
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.

Configuring a Port Connected to a Cisco 7960 IP Phone

Because a Cisco 7960 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.

These sections contain this configuration information:

- Configuring Cisco IP Phone Voice Traffic, page 12-5
- Configuring the Priority of Incoming Data Frames, page 12-7

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).

Beginning in privileged EXEC mode, follow these steps to configure voice traffic on a port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the interface connected to the phone, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>mls qos trust cos</td>
<td>Configure 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>
</tbody>
</table>

Note Before configuring the port trust state, you must first globally enable QoS by using the mls qos global configuration command.
### Chapter 12  Configuring Voice VLAN

**Configuring Voice VLAN**

This example shows how to configure a port connected to a Cisco IP Phone to use the CoS value to classify incoming traffic, to use IEEE 802.1p priority tagging for voice traffic, and to use the default native VLAN (VLAN 0) to carry all traffic:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust cos
Switch(config-if)# mls qos trust dot1p
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

To return the port to its default setting, use the `no switchport voice detect cisco-phone [full-duplex]` command.

This example shows how to enable `switchport voice detect` on a Cisco IP Phone:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport voice?
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport voice {detect cisco-phone [full-duplex]</td>
<td>vlan {vlan-id</td>
</tr>
<tr>
<td></td>
<td>• detect—Configure the interface to detect and recognize a Cisco IP phone.</td>
</tr>
<tr>
<td></td>
<td>• cisco-phone—When you initially implement the switchport voice detect command, this is the only allowed option. The default is no switchport voice detect cisco-phone [full-duplex].</td>
</tr>
<tr>
<td></td>
<td>• full-duplex—(Optional) Configure the switch to only accept a full-duplex Cisco IP phone.</td>
</tr>
<tr>
<td></td>
<td>Note Before configuring the switch port to detect and recognize a Cisco IP phone, confirm that the phone is powered by PoE. The configuration fails when power is provided by an AC source.</td>
</tr>
<tr>
<td></td>
<td>• vlan-id—Configure 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>• dot1p—Configure the phone to use IEEE 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. By default, the Cisco IP Phone forwards the voice traffic with an IEEE 802.1p priority of 5.</td>
</tr>
<tr>
<td></td>
<td>• none—Allow the phone to use its own configuration to send untagged voice traffic.</td>
</tr>
<tr>
<td></td>
<td>• untagged—Configure the phone to send untagged voice traffic.</td>
</tr>
</tbody>
</table>

**Step 4**

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
interface gigabitethernet0/1
```

```
mls qos trust cos
```

```
switchport voice vlan dot1p
```

```
end
```

To return the port to its default setting, use the `no switchport voice detect cisco-phone [full-duplex]` command.

**Step 5**

```
end
```

Return to privileged EXEC mode.

**Step 6**

```
show interfaces interface-id
```

```
switchport
```

```
show running-config interface interface-id
```

Verify your voice VLAN entries.

Verify your QoS and voice VLAN entries.

**Step 7**

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

(Optional) Save your entries in the configuration file.
Chapter 12      Configuring Voice VLAN

Configuring Voice VLAN

detect      detection enhancement keyword
vlan    VLAN for voice traffic
Switch(config-if)# switchport voice detect?
cisco-phone Cisco IP Phone
Switch(config-if)# switchport voice detect cisco-phone?
full-duplex full duplex keyword

Switch(config-if)# switchport voice detect cisco-phone full-duplex
end

This example shows how to disable switchport voice detect on a Cisco IP Phone:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 0/1
Switch(config-if)# no switchport voice detect cisco-phone
Switch(config-if)# no switchport voice detect cisco-phone full-duplex

Configuring the Priority of Incoming Data Frames

You can connect a PC or other data device to a Cisco IP Phone port. To process tagged data traffic (in IEEE 802.1Q or IEEE 802.1p frames), you can configure the switch to send CDP packets to instruct the phone how to send data packets from the device attached to the access port on the Cisco IP Phone. The PC can generate packets with an assigned CoS value. You can configure the phone to not change (trust) or to override (not trust) the priority of frames arriving on the phone port from connected devices.

Beginning in privileged EXEC mode, follow these steps to set the priority of data traffic received from the nonvoice port on the Cisco IP Phone:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface connected to the Cisco IP Phone, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| 3    | switchport priority extend {cos value | trust} | Set the priority of data traffic received from the Cisco IP Phone access port:  
  - cos value—Configure the phone to override the priority received from the PC or the attached device with the specified CoS value. The value is a number from 0 to 7, with 7 as the highest priority. The default priority is cos 0.  
  - trust—Configure the phone access port to trust the priority received from the PC or the attached device. |
| 4    | end | Return to privileged EXEC mode. |
| 5    | show interfaces interface-id switchport | Verify your entries. |
| 6    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

This example shows how to configure a port connected to a Cisco IP Phone to not change the priority of frames received from the PC or the attached device:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
To display voice VLAN configuration for an interface, use the `show interfaces interface-id switchport` privileged EXEC command.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

To return the port to its default setting, use the `no switchport priority extend` interface configuration command.

**Displaying Voice VLAN**

To display voice VLAN configuration for an interface, use the `show interfaces interface-id switchport` privileged EXEC command.
Configuring Private VLANs

This chapter describes how to configure private VLANs on the Catalyst 3560 switch.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter consists of these sections:

- Understanding Private VLANs, page 15-1
- Configuring Private VLANs, page 15-5
- Monitoring Private VLANs, page 15-14

Note

When you configure private VLANs, the switch must be in VTP transparent mode. See Chapter 14, “Configuring VTP.”

Understanding Private VLANs

The private-VLAN feature addresses two problems that service providers face when using VLANs:

- Scalability: The switch supports up to 1005 active VLANs. If a service provider assigns one VLAN per customer, this limits the numbers of customers that the service provider can support.
- To enable IP routing, each VLAN is assigned a subnet address space or a block of addresses, which can waste the unused IP addresses and cause IP address management problems.

Using private VLANs addresses the scalability problem and provides IP address management benefits for service providers and Layer 2 security for customers.

Private VLANs partition a regular VLAN domain into subdomains and can have multiple VLAN pairs—one for each subdomain. A subdomain is represented by a primary VLAN and a secondary VLAN.

All VLAN pairs in a private VLAN share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. See Figure 15-1.
Understanding Private VLANs

There are two types of secondary VLANs:

- Isolated VLANs—Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.

- Community VLANs—Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level.

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. Private-VLAN ports are access ports that are one of these types:

- Promiscuous—A promiscuous port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports that belong to the secondary VLANs associated with the primary VLAN.

- Isolated—An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN, except for the promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.

- Community—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities and from isolated ports within their private VLAN.

Note: Trunk ports carry traffic from regular VLANs and also from primary, isolated, and community VLANs.
Primary and secondary VLANs have these characteristics:

- **Primary VLAN**—A private VLAN has only one primary VLAN. Every port in a private VLAN is a member of the primary VLAN. The primary VLAN carries unidirectional traffic downstream from the promiscuous ports to the (isolated and community) host ports and to other promiscuous ports.

- **Isolated VLAN**—A private VLAN has only one isolated VLAN. An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway.

- **Community VLAN**—A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port gateways and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN.

A promiscuous port can serve only one primary VLAN, one isolated VLAN, and multiple community VLANs. Layer 3 gateways are typically connected to the switch through a promiscuous port. With a promiscuous port, you can connect a wide range of devices as access points to a private VLAN. For example, you can use a promiscuous port to monitor or back up all the private-VLAN servers from an administration workstation.

In a switched environment, you can assign an individual private VLAN and associated IP subnet to each individual or common group of end stations. The end stations need to communicate only with a default gateway to communicate outside the private VLAN.

You can use private VLANs to control access to end stations in these ways:

- Configure selected interfaces connected to end stations as isolated ports to prevent any Layer 2 communication and prevent Layer 2 communication at Layer 2. For example, the end stations are servers, this configuration prevents Layer 2 communication between the servers.

- Configure interfaces connected to default gateways and selected end stations (for example, backup servers) as promiscuous ports to allow all end stations access to a default gateway.

You can extend private VLANs across multiple devices by trunking the primary, isolated, and community VLANs to other devices that support private VLANs. To maintain the security of your private-VLAN configuration and to avoid other use of the VLANs configured as private VLANs, configure private VLANs on all intermediate devices, including devices that have no private-VLAN ports.

### IP Addressing Scheme with Private VLANs

Assigning a separate VLAN to each customer creates an inefficient IP addressing scheme:

- Assigning a block of addresses to a customer VLAN can result in unused IP addresses.

- If the number of devices in the VLAN increases, the number of assigned address might not be large enough to accommodate them.

These problems are reduced by using private VLANs, where all members in the private VLAN share a common address space, which is allocated to the primary VLAN. Hosts are connected to secondary VLANs, and the DHCP server assigns them IP addresses from the block of addresses allocated to the primary VLAN. Subsequent IP addresses can be assigned to customer devices in different secondary VLANs, but in the same primary VLAN. When new devices are added, the DHCP server assigns them the next available address from a large pool of subnet addresses.
Private VLANs across Multiple Switches

As with regular VLANs, private VLANs can span multiple switches. A trunk port carries the primary VLAN and secondary VLANs to a neighboring switch. The trunk port treats the private VLAN as any other VLAN. A feature of private VLANs across multiple switches is that traffic from an isolated port in switch A does not reach an isolated port on Switch B. See Figure 15-2.

Figure 15-2  Private VLANs across Switches

VLAN 100 = Primary VLAN
VLAN 201 = Secondary isolated VLAN
VLAN 202 = Secondary community VLAN

Because VTP does not support private VLANs, you must manually configure private VLANs on all switches in the Layer 2 network. If you do not configure the primary and secondary VLAN associations in some switches in the network, the Layer 2 databases in these switches are not merged. This can result in unnecessary flooding of private-VLAN traffic on those switches.

Note
When configuring private VLANs on the switch, always use the default Switch Database Management (SDM) template to balance system resources between unicast routes and Layer 2 entries. If another SDM template is configured, use the `sdm prefer default` global configuration command to set the default template. See Chapter 7, “Configuring SDM Templates.”

Private-VLAN Interaction with Other Features

Private VLANs have specific interaction with some other features, described in these sections:

- Private VLANs and Unicast, Broadcast, and Multicast Traffic, page 15-5
- Private VLANs and SVIs, page 15-5

You should also see the “Secondary and Primary VLAN Configuration” section on page 15-7 and the “Private-VLAN Configuration Guidelines” section.
Private VLANs and Unicast, Broadcast, and Multicast Traffic

In regular VLANs, devices in the same VLAN can communicate with each other at the Layer 2 level, but devices connected to interfaces in different VLANs must communicate at the Layer 3 level. In private VLANs, the promiscuous ports are members of the primary VLAN, while the host ports belong to secondary VLANs. Because the secondary VLAN is associated to the primary VLAN, members of these VLANs can communicate with each other at the Layer 2 level.

In a regular VLAN, broadcasts are forwarded to all ports in that VLAN. Private VLAN broadcast forwarding depends on the port sending the broadcast:

- An isolated port sends a broadcast only to the promiscuous ports or trunk ports.
- A community port sends a broadcast to all promiscuous ports, trunk ports, and ports in the same community VLAN.
- A promiscuous port sends a broadcast to all ports in the private VLAN (other promiscuous ports, trunk ports, isolated ports, and community ports).

Multicast traffic is routed or bridged across private-VLAN boundaries and within a single community VLAN. Multicast traffic is not forwarded between ports in the same isolated VLAN or between ports in different secondary VLANs.

Private VLANs and SVIs

In a Layer 3 switch, a switch virtual interface (SVI) represents the Layer 3 interface of a VLAN. Layer 3 devices communicate with a private VLAN only through the primary VLAN and not through secondary VLANs. Configure Layer 3 VLAN interfaces only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

- If you try to configure a VLAN with an active SVI as a secondary VLAN, the configuration is not allowed until you disable the SVI.
- If you try to create an SVI on a VLAN that is configured as a secondary VLAN and the secondary VLAN is already mapped at Layer 3, the SVI is not created, and an error is returned. If the SVI is not mapped at Layer 3, the SVI is created, but it is automatically shut down.

When the primary VLAN is associated with and mapped to the secondary VLAN, any configuration on the primary VLAN is propagated to the secondary VLAN SVIs. For example, if you assign an IP subnet to the primary VLAN SVI, this subnet is the IP subnet address of the entire private VLAN.

Configuring Private VLANs

These sections contain this configuration information:

- **Tasks for Configuring Private VLANs**, page 15-6
- **Default Private-VLAN Configuration**, page 15-6
- **Private-VLAN Configuration Guidelines**, page 15-6
- **Configuring and Associating VLANs in a Private VLAN**, page 15-9
- **Configuring a Layer 2 Interface as a Private-VLAN Host Port**, page 15-11
- **Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port**, page 15-12
- **Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface**, page 15-13
Tasks for Configuring Private VLANs

To configure a private VLAN, follow these steps:

Step 1  Set VTP mode to transparent.
Step 2  Create the primary and secondary VLANs and associate them. See the “Configuring and Associating
VLANs in a Private VLAN” section on page 15-9.

Note  If the VLAN is not created already, the private-VLAN configuration process creates it.

Step 3  Configure interfaces to be isolated or community host ports, and assign VLAN membership to the host
port. See the “Configuring a Layer 2 Interface as a Private-VLAN Host Port” section on page 15-11.
Step 4  Configure interfaces as promiscuous ports, and map the promiscuous ports to the primary-secondary
VLAN pair. See the “Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port” section on
page 15-12.
Step 5  If inter-VLAN routing will be used, configure the primary SVI, and map secondary VLANs to the
primary. See the “Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface” section on
Step 6  Verify private-VLAN configuration.

Default Private-VLAN Configuration

No private VLANs are configured.

Private-VLAN Configuration Guidelines

Guidelines for configuring private VLANs fall into these categories:

- Secondary and Primary VLAN Configuration, page 15-7
- Private-VLAN Port Configuration, page 15-8
- Limitations with Other Features, page 15-8
Secondary and Primary VLAN Configuration

Follow these guidelines when configuring private VLANs:

- If the switch is running VTP version 1 or 2, you must set VTP to transparent mode. After you configure a private VLAN, you should not change the VTP mode to client or server. For information about VTP, see Chapter 14, “Configuring VTP.” VTP version 3 supports private VLANs in all modes.

- With VTP version 1 or 2, after you have configured private VLANs, use the `copy running-config startup config` privileged EXEC command to save the VTP transparent mode configuration and private-VLAN configuration in the switch startup configuration file. Otherwise, if the switch resets, it defaults to VTP server mode, which does not support private VLANs. VTP version 3 does support private VLANs.

- VTP version 1 and 2 do not propagate private-VLAN configuration. You must configure private VLANs on each device where you want private-VLAN ports unless the devices are running VTP version 3.

- You cannot configure VLAN 1 or VLANs 1002 to 1005 as primary or secondary VLANs. Extended VLANs (VLAN IDs 1006 to 4094) can belong to private VLANs.

- A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it. An isolated or community VLAN can have only one primary VLAN associated with it.

- Although a private VLAN contains more than one VLAN, only one Spanning Tree Protocol (STP) instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

- You can enable DHCP snooping on private VLANs. When you enable DHCP snooping on the primary VLAN, it is propagated to the secondary VLANs. If you configure DHCP on a secondary VLAN, the configuration does not take effect if the primary VLAN is already configured.

- When you enable IP source guard on private-VLAN ports, you must enable DHCP snooping on the primary VLAN.

- We recommend that you prune the private VLANs from the trunks on devices that carry no traffic in the private VLANs.

- You can apply different quality of service (QoS) configurations to primary, isolated, and community VLANs.

- Sticky ARP
  - Sticky ARP entries are those learned on SVIs and Layer 3 interfaces. They entries do not age out.
  - The `ip sticky-arp` global configuration command is supported only on SVIs belonging to private VLANs.
  - The `ip sticky-arp` interface configuration command is only supported on Layer 3 interfaces
    - SVIs belonging to normal VLANs
    - SVIs belonging to private VLANs

For more information about using the `ip sticky-arp` global configuration and the `ip sticky-arp interface` configuration commands, see the command reference for this release.

- You can configure VLAN maps on primary and secondary VLANs (see the “Configuring VLAN Maps” section on page 33-29). However, we recommend that you configure the same VLAN maps on private-VLAN primary and secondary VLANs.
When a frame is Layer-2 forwarded within a private VLAN, the same VLAN map is applied at the ingress side and at the egress side. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the ingress side.

- For frames going upstream from a host port to a promiscuous port, the VLAN map configured on the secondary VLAN is applied.
- For frames going downstream from a promiscuous port to a host port, the VLAN map configured on the primary VLAN is applied.

To filter out specific IP traffic for a private VLAN, you should apply the VLAN map to both the primary and secondary VLANs.

You can apply router ACLs only on the primary-VLAN SVIs. The ACL is applied to both primary and secondary VLAN Layer 3 traffic.

Although private VLANs provide host isolation at Layer 2, hosts can communicate with each other at Layer 3.

Private VLANs support these Switched Port Analyzer (SPAN) features:
- You can configure a private-VLAN port as a SPAN source port.
- You can use VLAN-based SPAN (VSPAN) on primary, isolated, and community VLANs or use SPAN on only one VLAN to separately monitor egress or ingress traffic.

### Private-VLAN Port Configuration

Follow these guidelines when configuring private-VLAN ports:

- Use only the private-VLAN configuration commands to assign ports to primary, isolated, or community VLANs. Layer 2 access ports assigned to the VLANs that you configure as primary, isolated, or community VLANs are inactive while the VLAN is part of the private-VLAN configuration. Layer 2 trunk interfaces remain in the STP forwarding state.
- Do not configure ports that belong to a PAgP or LACP EtherChannel as private-VLAN ports. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.
- Enable Port Fast and BPDU guard on isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence (see Chapter 18, “Configuring Optional Spanning-Tree Features”). When enabled, STP applies the BPDU guard feature to all Port Fast-configured Layer 2 LAN ports. Do not enable Port Fast and BPDU guard on promiscuous ports.
- If you delete a VLAN used in the private-VLAN configuration, the private-VLAN ports associated with the VLAN become inactive.
- Private-VLAN ports can be on different network devices if the devices are trunk-connected and the primary and secondary VLANs have not been removed from the trunk.

### Limitations with Other Features

When configuring private VLANs, remember these limitations with other features:

- Do not configure fallback bridging on switches with private VLANs.
- When IGMP snooping is enabled on the switch (the default), the switch supports no more than 20 private-VLAN domains.
Chapter 15  Configuring Private VLANs

Configuring Private VLANs

- Do not configure a remote SPAN (RSPAN) VLAN as a private-VLAN primary or secondary VLAN. For more information about SPAN, see Chapter 28, “Configuring SPAN and RSPAN.”
- Do not configure private-VLAN ports on interfaces configured for these other features:
  - dynamic-access port VLAN membership
  - Dynamic Trunking Protocol (DTP)
  - Port Aggregation Protocol (PAgP)
  - Link Aggregation Control Protocol (LACP)
  - Multicast VLAN Registration (MVR)
  - voice VLAN
  - Web Cache Communication Protocol (WCCP)
- A private-VLAN port cannot be a secure port and should not be configured as a protected port.
- You can configure IEEE 802.1x port-based authentication on a private-VLAN port, but do not configure IEEE 802.1x with port security, voice VLAN, or per-user ACL on private-VLAN ports.
- A private-VLAN host or promiscuous port cannot be a SPAN destination port. If you configure a SPAN destination port as a private-VLAN port, the port becomes inactive.
- If you configure a static MAC address on a promiscuous port in the primary VLAN, you must add the same static address to all associated secondary VLANs. If you configure a static MAC address on a host port in a secondary VLAN, you must add the same static MAC address to the associated primary VLAN. When you delete a static MAC address from a private-VLAN port, you must remove all instances of the configured MAC address from the private VLAN.

Note: Dynamic MAC addresses learned in one VLAN of a private VLAN are replicated in the associated VLANs. For example, a MAC address learned in a secondary VLAN is replicated in the primary VLAN. When the original dynamic MAC address is deleted or aged out, the replicated addresses are removed from the MAC address table.

- Configure Layer 3 VLAN interfaces only for primary VLANs.

Configuring and Associating VLANs in a Private VLAN

Beginning in privileged EXEC mode, follow these steps to configure a private VLAN:

Note: The private-vlan commands do not take effect until you exit VLAN configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 vtp mode transparent</td>
<td>Set VTP mode to transparent (disable VTP).</td>
</tr>
<tr>
<td>Step 3 vlan vlan-id</td>
<td>Enter VLAN configuration mode and designate or create a VLAN that will be the primary VLAN. The VLAN ID range is 2 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>Step 4 private-vlan primary</td>
<td>Designate the VLAN as the primary VLAN.</td>
</tr>
</tbody>
</table>
When you associate secondary VLANs with a primary VLAN, note this syntax information:

- The `secondary_vlan_list` parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- The `secondary_vlan_list` parameter can contain multiple community VLAN IDs but only one isolated VLAN ID.
- Enter a `secondary_vlan_list`, or use the `add` keyword with a `secondary_vlan_list` to associate secondary VLANs with a primary VLAN.
- Use the `remove` keyword with a `secondary_vlan_list` to clear the association between secondary VLANs and a primary VLAN.
- The command does not take effect until you exit VLAN configuration mode.

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, to associate them in a private VLAN, and to verify the configuration:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
```
Chapter 15  Configuring Private VLANs

Configuring Private VLANs

Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
Switch(config)# show vlan private vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
20      501       isolated
20      502       community
20      503       community
20      504       non-operational

Configuring a Layer 2 Interface as a Private-VLAN Host Port

Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN host port and to associate it with primary and secondary VLANs:

Command | Purpose
---|---
Step 1 configure terminal | Enter global configuration mode.
Step 2 interface interface-id | Enter interface configuration mode for the Layer 2 interface to be configured.
Step 3 switchport mode private-vlan host | Configure the Layer 2 port as a private-VLAN host port.
Step 4 switchport private-vlan host-association primary_vlan_id secondary_vlan_id | Associate the Layer 2 port with a private VLAN.
Step 5 end | Return to privileged EXEC mode.
Step 6 show interfaces [interface-id] switchport | Verify the configuration.
Step 7 copy running-config startup config | (Optional) Save your entries in the switch startup configuration file.

This example shows how to configure an interface as a private-VLAN host port, associate it with a private-VLAN pair, and verify the configuration:

Switch# configure terminal
Switch(config)# interface gigabitethernet0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 25
Switch(config-if)# end
Switch# show interfaces gigabitethernet0/22 switchport
Name: Gi0/22
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 20 (VLAN0020) 25 (VLAN0025)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
  20 (VLAN0020) 25 (VLAN0025)

<output truncated>

### Configuring a Layer 2 Interface as a Private-VLAN Promiscuous Port

Beginning in privileged EXEC mode, follow these steps to configure a Layer 2 interface as a private-VLAN promiscuous port and map it to primary and secondary VLANs:

#### Note

Isolated and community VLANs are both secondary VLANs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode private-vlan promiscuous</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport private-vlan mapping primary_vlan_id {add</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show interfaces [interface-id] switchport</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup config</td>
</tr>
</tbody>
</table>

When you configure a Layer 2 interface as a private-VLAN promiscuous port, note this syntax information:

- The `secondary_vlan_list` parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- Enter a `secondary_vlan_list`, or use the `add` keyword with a `secondary_vlan_list` to map the secondary VLANs to the private-VLAN promiscuous port.
- Use the `remove` keyword with a `secondary_vlan_list` to clear the mapping between secondary VLANs and the private-VLAN promiscuous port.
This example shows how to configure an interface as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```bash
Switch# configure terminal
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

Use the `show vlan private-vlan` or the `show interface status` privileged EXEC command to display primary and secondary VLANs and private-VLAN ports on the switch.

### Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface

If the private VLAN will be used for inter-VLAN routing, you configure an SVI for the primary VLAN and map secondary VLANs to the SVI.

**Note**

Isolated and community VLANs are both secondary VLANs.

Beginning in privileged EXEC mode, follow these steps to map secondary VLANs to the SVI of a primary VLAN to allow Layer 3 switching of private-VLAN traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface vlan primary_vlan_id</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`private-vlan mapping [add</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>show interface private-vlan mapping</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>copy running-config startup config</code></td>
</tr>
</tbody>
</table>

**Note**

The `private-vlan mapping` interface configuration command only affects private-VLAN traffic that is switched through Layer 3.

When you map secondary VLANs to the Layer 3 VLAN interface of a primary VLAN, note this syntax information:

- The `secondary_vlan_list` parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs.
- Enter a `secondary_vlan_list`, or use the `add` keyword with a `secondary_vlan_list` to map the secondary VLANs to the primary VLAN.
- Use the `remove` keyword with a `secondary_vlan_list` to clear the mapping between secondary VLANs and the primary VLAN.
Chapter 15      Configuring Private VLANs

Monitoring Private VLANs

This example shows how to map the interfaces of VLANs 501 and 502 to primary VLAN 10, which permits routing of secondary VLAN ingress traffic from private VLANs 501 to 502:

Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# private-vlan mapping 501-502
Switch(config-if)# end
Switch# show interfaces private-vlan mapping

<table>
<thead>
<tr>
<th>Interface</th>
<th>Secondary VLAN</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan10</td>
<td>501</td>
<td>isolated</td>
</tr>
<tr>
<td>vlan10</td>
<td>502</td>
<td>community</td>
</tr>
</tbody>
</table>

This is an example of the output from the `show vlan private-vlan` command:

Switch(config)# show vlan private-vlan

<table>
<thead>
<tr>
<th>Primary</th>
<th>Secondary</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>501</td>
<td>isolated</td>
<td>Fa0/1, Gi0/1, Gi0/3</td>
</tr>
<tr>
<td>10</td>
<td>502</td>
<td>community</td>
<td>Fa0/11, Gi0/1, Gi0/4</td>
</tr>
<tr>
<td>10</td>
<td>503</td>
<td>non-operational</td>
<td></td>
</tr>
</tbody>
</table>

Table 15-1    Private VLAN Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces status</td>
<td>Displays the status of interfaces, including the VLANs to which they belongs.</td>
</tr>
<tr>
<td>show vlan private-vlan [type]</td>
<td>Display the private-VLAN information for the switch.</td>
</tr>
<tr>
<td>show interface switchport</td>
<td>Display the private-VLAN configuration on interfaces.</td>
</tr>
<tr>
<td>show interface private-vlan mapping</td>
<td>Display information about the private-VLAN mapping for VLAN SVIs.</td>
</tr>
</tbody>
</table>
Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. Tunneling is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. The Catalyst 3560 switch supports IEEE 802.1Q tunneling and Layer 2 protocol tunneling.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter contains these sections:
- Understanding IEEE 802.1Q Tunneling, page 16-1
- Configuring IEEE 802.1Q Tunneling, page 16-4
- Understanding Layer 2 Protocol Tunneling, page 16-7
- Configuring Layer 2 Protocol Tunneling, page 16-10
- Monitoring and Maintaining Tunneling Status, page 16-18

Understanding IEEE 802.1Q Tunneling

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

Using the IEEE 802.1Q tunneling feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using IEEE 802.1Q tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support IEEE 802.1Q tunneling is called a tunnel port. When you configure tunneling, you assign a tunnel port to a VLAN ID that is dedicated to tunneling. Each customer requires a separate service-provider VLAN ID, but that VLAN ID supports all of the customer’s VLANs.
Customer traffic tagged in the normal way with appropriate VLAN IDs comes from an IEEE 802.1Q trunk port on the customer device and into a tunnel port on the service-provider edge switch. The link between the customer device and the edge switch is asymmetric because one end is configured as an IEEE 802.1Q trunk port, and the other end is configured as a tunnel port. You assign the tunnel port interface to an access VLAN ID that is unique to each customer. See Figure 16-1.

Figure 16-1  IEEE 802.1Q Tunnel Ports in a Service-Provider Network

Packets coming from the customer trunk port into the tunnel port on the service-provider edge switch are normally IEEE 802.1Q-tagged with the appropriate VLAN ID. The tagged packets remain intact inside the switch and when they exit the trunk port into the service-provider network, they are encapsulated with another layer of an IEEE 802.1Q tag (called the metro tag) that contains the VLAN ID that is unique to the customer. The original customer IEEE 802.1Q tag is preserved in the encapsulated packet. Therefore, packets entering the service-provider network are double-tagged, with the outer (metro) tag containing the customer’s access VLAN ID, and the inner VLAN ID being that of the incoming traffic.

When the double-tagged packet enters another trunk port in a service-provider core switch, the outer tag is stripped as the switch processes the packet. When the packet exits another trunk port on the same core switch, the same metro tag is again added to the packet. Figure 16-2 shows the tag structures of the double-tagged packets.

Note

Remove the Layer 2 protocol configuration from a trunk port because incoming encapsulated packets change that trunk port to error disabled. The outgoing encapsulated VTP (CDP and STP) packets are dropped on that trunk.
When the packet enters the trunk port of the service-provider egress switch, the outer tag is again stripped as the switch internally processes the packet. However, the metro tag is not added when the packet is sent out the tunnel port on the edge switch into the customer network. The packet is sent as a normal IEEE 802.1Q-tagged frame to preserve the original VLAN numbers in the customer network.

In Figure 16-1, Customer A was assigned VLAN 30, and Customer B was assigned VLAN 40. Packets entering the edge switch tunnel ports with IEEE 802.1Q tags are double-tagged when they enter the service-provider network, with the outer tag containing VLAN ID 30 or 40, appropriately, and the inner tag containing the original VLAN number, for example, VLAN 100. Even if both Customers A and B have VLAN 100 in their networks, the traffic remains segregated within the service-provider network because the outer tag is different. Each customer controls its own VLAN numbering space, which is independent of the VLAN numbering space used by other customers and the VLAN numbering space used by the service-provider network.

At the outbound tunnel port, the original VLAN numbers on the customer’s network are recovered. It is possible to have multiple levels of tunneling and tagging, but the switch supports only one level in this release.

If traffic coming from a customer network is not tagged (native VLAN frames), these packets are bridged or routed as normal packets. All packets entering the service-provider network through a tunnel port on an edge switch are treated as untagged packets, whether they are untagged or already tagged with IEEE 802.1Q headers. The packets are encapsulated with the metro tag VLAN ID (set to the access VLAN of the tunnel port) when they are sent through the service-provider network on an IEEE 802.1Q trunk port. The priority field on the metro tag is set to the interface class of service (CoS) priority configured on the tunnel port. (The default is zero if none is configured.)
Configuring IEEE 802.1Q Tunneling

These sections contain this configuration information:

- Default IEEE 802.1Q Tunneling Configuration, page 16-4
- IEEE 802.1Q Tunneling Configuration Guidelines, page 16-4
- IEEE 802.1Q Tunneling and Other Features, page 16-6
- Configuring an IEEE 802.1Q Tunneling Port, page 16-6

Default IEEE 802.1Q Tunneling Configuration

By default, IEEE 802.1Q tunneling is disabled because the default switchport mode is dynamic auto. Tagging of IEEE 802.1Q native VLAN packets on all IEEE 802.1Q trunk ports is also disabled.

IEEE 802.1Q Tunneling Configuration Guidelines

When you configure IEEE 802.1Q tunneling, you should always use an asymmetrical link between the customer device and the edge switch, with the customer device port configured as an IEEE 802.1Q trunk port and the edge switch port configured as a tunnel port.

Assign tunnel ports only to VLANs that are used for tunneling.

Configuration requirements for native VLANs and for and maximum transmission units (MTUs) are explained in these next sections.

Native VLANs

When configuring IEEE 802.1Q tunneling on an edge switch, you must use IEEE 802.1Q trunk ports for sending packets into the service-provider network. However, packets going through the core of the service-provider network can be carried through IEEE 802.1Q trunks, ISL trunks, or nontrunking links. When IEEE 802.1Q trunks are used in these core switches, the native VLANs of the IEEE 802.1Q trunks must not match any native VLAN of the nontrunking (tunneling) port on the same switch because traffic on the native VLAN would not be tagged on the IEEE 802.1Q sending trunk port.

See Figure 16-3. VLAN 40 is configured as the native VLAN for the IEEE 802.1Q trunk port from Customer X at the ingress edge switch in the service-provider network (Switch B). Switch A of Customer X sends a tagged packet on VLAN 30 to the ingress tunnel port of Switch B in the service-provider network, which belongs to access VLAN 40. Because the access VLAN of the tunnel port (VLAN 40) is the same as the native VLAN of the edge-switch trunk port (VLAN 40), the metro tag is not added to tagged packets received from the tunnel port. The packet carries only the VLAN 30 tag through the service-provider network to the trunk port of the egress-edge switch (Switch C) and is misdirected through the egress switch tunnel port to Customer Y.
These are some ways to solve this problem:

- Use ISL trunks between core switches in the service-provider network. Although customer interfaces connected to edge switches must be IEEE 802.1Q trunks, we recommend using ISL trunks for connecting switches in the core layer.

- Use the `vlan dot1q tag native` global configuration command to configure the edge switch so that all packets going out an IEEE 802.1Q trunk, including the native VLAN, are tagged. If the switch is configured to tag native VLAN packets on all IEEE 802.1Q trunks, the switch accepts untagged packets, but sends only tagged packets.

- Ensure that the native VLAN ID on the edge-switch trunk port is not within the customer VLAN range. For example, if the trunk port carries traffic of VLANs 100 to 200, assign the native VLAN a number outside that range.

![Figure 16-3 Potential Problem with IEEE 802.1Q Tunneling and Native VLANs](image)

**System MTU**

The default system MTU for traffic on the switch is 1500 bytes. You can configure Fast Ethernet ports to support frames larger than 1500 bytes by using the `system mtu` global configuration command. You can configure Gigabit Ethernet ports to support frames larger than 1500 bytes by using the `system mtu jumbo` global configuration command. Because the IEEE 802.1Q tunneling feature increases the frame size by 4 bytes when the metro tag is added, you must configure all switches in the service-provider network to be able to process maximum frames by increasing the switch system MTU size to at least 1504 bytes. The maximum allowable system MTU for Gigabit Ethernet interfaces is 9000 bytes; the maximum system MTU for Fast Ethernet interfaces is 1998 bytes.
IEEE 802.1Q Tunneling and Other Features

Although IEEE 802.1Q tunneling works well for Layer 2 packet switching, there are incompatibilities between some Layer 2 features and Layer 3 switching.

- A tunnel port cannot be a routed port.
- IP routing is not supported on a VLAN that includes IEEE 802.1Q ports. Packets received from a tunnel port are forwarded based only on Layer 2 information. If routing is enabled on a switch virtual interface (SVI) that includes tunnel ports, untagged IP packets received from the tunnel port are recognized and routed by the switch. Customer can access the internet through its native VLAN. If this access is not needed, you should not configure SVIs on VLANs that include tunnel ports.
- Fallback bridging is not supported on tunnel ports. Because all IEEE 802.1Q-tagged packets received from a tunnel port are treated as non-IP packets, if fallback bridging is enabled on VLANs that have tunnel ports configured, IP packets would be improperly bridged across VLANs. Therefore, you must not enable fallback bridging on VLANs with tunnel ports.
- Tunnel ports do not support IP access control lists (ACLs).
- Layer 3 quality of service (QoS) ACLs and other QoS features related to Layer 3 information are not supported on tunnel ports. MAC-based QoS is supported on tunnel ports.
- EtherChannel port groups are compatible with tunnel ports as long as the IEEE 802.1Q configuration is consistent within an EtherChannel port group.
- Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), and UniDirectional Link Detection (UDLD) are supported on IEEE 802.1Q tunnel ports.
- Dynamic Trunking Protocol (DTP) is not compatible with IEEE 802.1Q tunneling because you must manually configure asymmetric links with tunnel ports and trunk ports.
- VLAN Trunking Protocol (VTP) does not work between devices that are connected by an asymmetrical link or devices that communicate through a tunnel.
- Loopback detection is supported on IEEE 802.1Q tunnel ports.
- When a port is configured as an IEEE 802.1Q tunnel port, spanning-tree bridge protocol data unit (BPDU) filtering is automatically enabled on the interface. Cisco Discovery Protocol (CDP) and the Layer Link Discovery Protocol (LLDP) are automatically disabled on the interface.

Configuring an IEEE 802.1Q Tunneling Port

Beginning in privileged EXEC mode, follow these steps to configure a port as an IEEE 802.1Q tunnel port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Enter interface configuration mode for the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces include physical interfaces and port-channel logical interfaces (port channels 1 to 48).</td>
</tr>
<tr>
<td>switchport access vlan vlan-id</td>
<td>Specify the default VLAN, which is used if the interface stops trunking. This VLAN ID is specific to the particular customer.</td>
</tr>
<tr>
<td>switchport mode dot1q-tunnel</td>
<td>Set the interface as an IEEE 802.1Q tunnel port.</td>
</tr>
</tbody>
</table>
Chapter 16      Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Understanding Layer 2 Protocol Tunneling

Customers at different sites connected across a service-provider network need to use various Layer 2 protocols to scale their topologies to include all remote sites, as well as the local sites. STP must run properly, and every VLAN should build a proper spanning tree that includes the local site and all remote sites across the service-provider network. Cisco Discovery Protocol (CDP) must discover neighboring Cisco devices from local and remote sites. VLAN Trunking Protocol (VTP) must provide consistent VLAN configuration throughout all sites in the customer network.

Use the **no switchport mode dot1q-tunnel** interface configuration command to return the port to the default state of dynamic desirable. Use the **no vlan dot1q tag native** global configuration command to disable tagging of native VLAN packets.

This example shows how to configure an interface as a tunnel port, enable tagging of native VLAN packets, and verify the configuration. In this configuration, the VLAN ID for the customer connected to Gigabit Ethernet interface 7 is VLAN 22.

```
Switch(config)# interface gigabitethernet0/7
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet0/7
Port
-----
G10/1Port
-----
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> vlan dot1q tag native</td>
<td>(Optional) Set the switch to enable tagging of native VLAN packets on all IEEE 802.1Q trunk ports. When not set, and a customer VLAN ID is the same as the native VLAN, the trunk port does not apply a metro tag, and packets could be sent to the wrong destination.</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> show running-config</td>
<td>Display the ports configured for IEEE 802.1Q tunneling.</td>
</tr>
<tr>
<td>show dot1q-tunnel</td>
<td>Display the ports that are in tunnel mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong> show vlan dot1q tag native</td>
<td>Display IEEE 802.1Q native VLAN tagging status.</td>
</tr>
<tr>
<td><strong>Step 10</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Understanding Layer 2 Protocol Tunneling

When protocol tunneling is enabled, edge switches on the inbound side of the service-provider network encapsulate Layer 2 protocol packets with a special MAC address and send them across the service-provider network. Core switches in the network do not process these packets but forward them as normal packets. Layer 2 protocol data units (PDUs) for CDP, STP, or VTP cross the service-provider network and are delivered to customer switches on the outbound side of the service-provider network. Identical packets are received by all customer ports on the same VLANs with these results:

- Users on each of a customer’s sites can properly run STP, and every VLAN can build a correct spanning tree based on parameters from all sites and not just from the local site.
- CDP discovers and shows information about the other Cisco devices connected through the service-provider network.
- VTP provides consistent VLAN configuration throughout the customer network, propagating to all switches through the service provider.

To provide interoperability with third-party vendors, you can use the Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. You implement bypass mode by enabling Layer 2 protocol tunneling on the egress trunk port. When Layer 2 protocol tunneling is enabled on the trunk port, the encapsulated tunnel MAC address is removed and the protocol packets have their normal MAC address.

Layer 2 protocol tunneling can be used independently or can enhance IEEE 802.1Q tunneling. If protocol tunneling is not enabled on IEEE 802.1Q tunneling ports, remote switches at the receiving end of the service-provider network do not receive the PDUs and cannot properly run STP, CDP, and VTP. When protocol tunneling is enabled, Layer 2 protocols within each customer’s network are totally separate from those running within the service-provider network. Customer switches on different sites that send traffic through the service-provider network with IEEE 802.1Q tunneling achieve complete knowledge of the customer’s VLAN. If IEEE 802.1Q tunneling is not used, you can still enable Layer 2 protocol tunneling by connecting to the customer switch through access ports and by enabling tunneling on the service-provider access port.

For example, in Figure 16-4, Customer X has four switches in the same VLAN, that are connected through the service-provider network. If the network does not tunnel PDUs, switches on the far ends of the network cannot properly run STP, CDP, and VTP. For example, STP for a VLAN on a switch in Customer X, Site 1, will build a spanning tree on the switches at that site without considering convergence parameters based on Customer X’s switch in Site 2. This could result in the topology shown in Figure 16-5.
In an SP network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When you enable protocol tunneling (PAgP or LACP) on the SP switch, remote customer switches receive the PDUs and can negotiate the automatic creation of EtherChannels.
Configuring Layer 2 Protocol Tunneling

You can enable Layer 2 protocol tunneling (by protocol) on the ports that are connected to the customer in the edge switches of the service-provider network. The service-provider edge switches connected to the customer switch perform the tunneling process. Edge-switch tunnel ports are connected to customer IEEE 802.1Q trunk ports. Edge-switch access ports are connected to customer access ports. The edge switches connected to the customer switch perform the tunneling process.

You can enable Layer 2 protocol tunneling on ports that are configured as access ports or tunnel ports. You cannot enable Layer 2 protocol tunneling on ports configured in either switchport mode dynamic auto (the default mode) or switchport mode dynamic desirable.

The switch supports Layer 2 protocol tunneling for CDP, STP, and VTP. For emulated point-to-point network topologies, it also supports PAgP, LACP, and UDLD protocols. The switch does not support Layer 2 protocol tunneling for LLDP.

Caution

PAgP, LACP, and UDLD protocol tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

When the Layer 2 PDUs that entered the service-provider inbound edge switch through a Layer 2 protocol-enabled port exit through the trunk port into the service-provider network, the switch overwrites the customer PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0). If IEEE 802.1Q tunneling is enabled, packets are also double-tagged; the outer tag is the customer metro tag, and the inner tag is the customer’s VLAN tag. The core switches ignore the inner tags and forward the packet to all trunk ports in the same metro VLAN. The edge switches on the outbound side restore the proper Layer 2 protocol and MAC address information and forward the packets to all tunnel or access ports in the same metro VLAN. Therefore, the Layer 2 PDUs remain intact and are delivered across the service-provider infrastructure to the other side of the customer network.
See Figure 16-4, with Customer X and Customer Y in access VLANs 30 and 40, respectively. Asymmetric links connect the customers in Site 1 to edge switches in the service-provider network. The Layer 2 PDUs (for example, BPDUs) coming into Switch 2 from Customer Y in Site 1 are forwarded to the infrastructure as double-tagged packets with the well-known MAC address as the destination MAC address. These double-tagged packets have the metro VLAN tag of 40, as well as an inner VLAN tag (for example, VLAN 100). When the double-tagged packets enter Switch D, the outer VLAN tag 40 is removed, the well-known MAC address is replaced with the respective Layer 2 protocol MAC address, and the packet is sent to Customer Y on Site 2 as a single-tagged frame in VLAN 100.

You can also enable Layer 2 protocol tunneling on access ports on the edge switch connected to access or trunk ports on the customer switch. In this case, the encapsulation and decapsulation process is the same as described in the previous paragraph, except that the packets are not double-tagged in the service-provider network. The single tag is the customer-specific access VLAN tag.

These sections contain this configuration information:

- Default Layer 2 Protocol Tunneling Configuration, page 16-11
- Configuring Layer 2 Protocol Tunneling, page 16-13
- Configuring Layer 2 Tunneling for EtherChannels, page 16-14

## Default Layer 2 Protocol Tunneling Configuration

Table 16-1 shows the default Layer 2 protocol tunneling configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 protocol tunneling</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Shutdown threshold</td>
<td>None set.</td>
</tr>
<tr>
<td>Drop threshold</td>
<td>None set.</td>
</tr>
<tr>
<td>CoS value</td>
<td>If a CoS value is configured on the interface, that value is used to set the BPDU CoS value for Layer 2 protocol tunneling. If no CoS value is configured at the interface level, the default value for CoS marking of L2 protocol tunneling BPDUs is 5. This does not apply to data traffic.</td>
</tr>
</tbody>
</table>

## Layer 2 Protocol Tunneling Configuration Guidelines

These are some configuration guidelines and operating characteristics of Layer 2 protocol tunneling:

- The switch supports tunneling of CDP, STP, including multiple STP (MSTP), and VTP. Protocol tunneling is disabled by default but can be enabled for the individual protocols on IEEE 802.1Q tunnel ports or access ports.
- The switch does not support Layer 2 protocol tunneling on ports with switchport mode dynamic auto or dynamic desirable.
- DTP is not compatible with layer 2 protocol tunneling.
The edge switches on the outbound side of the service-provider network restore the proper Layer 2 protocol and MAC address information and forward the packets to all tunnel and access ports in the same metro VLAN.

For interoperability with third-party vendor switches, the switch supports a Layer 2 protocol-tunnel bypass feature. Bypass mode transparently forwards control PDUs to vendor switches that have different ways of controlling protocol tunneling. When Layer 2 protocol tunneling is enabled on ingress ports on a switch, egress trunk ports forward the tunneled packets with a special encapsulation. If you also enable Layer 2 protocol tunneling on the egress trunk port, this behavior is bypassed, and the switch forwards control PDUs without any processing or modification.

The switch supports PAgP, LACP, and UDLD tunneling for emulated point-to-point network topologies. Protocol tunneling is disabled by default but can be enabled for the individual protocols on IEEE 802.1Q tunnel ports or on access ports.

If you enable PAgP or LACP tunneling, we recommend that you also enable UDLD on the interface for faster link-failure detection.

EtherChannel port groups are compatible with tunnel ports when the IEEE 802.1Q configuration is consistent within an EtherChannel port group.

If an encapsulated PDU (with the proprietary destination MAC address) is received from a tunnel port or an access port with Layer 2 tunneling enabled, the tunnel port is shut down to prevent loops. The port also shuts down when a configured shutdown threshold for the protocol is reached. You can manually re-enable the port (by entering a `shutdown` and a `no shutdown` command sequence). If `errdisable` recovery is enabled, the operation is retried after a specified time interval.

Only decapsulated PDUs are forwarded to the customer network. The spanning-tree instance running on the service-provider network does not forward BPDUs to tunnel ports. CDP packets are not forwarded from tunnel ports.

When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, shutdown threshold for the PDUs generated by the customer network. If the limit is exceeded, the port shuts down. You can also limit BPDU rate by using QoS ACLs and policy maps on a tunnel port.

When protocol tunneling is enabled on an interface, you can set a per-protocol, per-port, drop threshold for the PDUs generated by the customer network. If the limit is exceeded, the port drops PDUs until the rate at which it receives them is below the drop threshold.

Because tunneled PDUs (especially STP BPDUs) must be delivered to all remote sites so that the customer virtual network operates properly, you can give PDUs higher priority within the service-provider network than data packets received from the same tunnel port. By default, the PDUs use the same CoS value as data packets.
Configuring Layer 2 Protocol Tunneling

Beginning in privileged EXEC mode, follow these steps to configure a port for Layer 2 protocol tunneling:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the service-provider network that connects to the customer switch. Valid interfaces can be physical interfaces and port-channel logical interfaces (port channels 1 to 48).</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode access</td>
<td>Configure the interface as an access port or an IEEE 802.1Q tunnel port.</td>
</tr>
<tr>
<td></td>
<td>switchport mode dot1q-tunnel</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>l2protocol-tunnel [cdp</td>
<td>stp</td>
</tr>
<tr>
<td>Step 5</td>
<td>l2protocol-tunnel shutdown-threshold [cdp</td>
<td>stp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.</td>
</tr>
<tr>
<td>Step 6</td>
<td>l2protocol-tunnel drop-threshold [cdp</td>
<td>stp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.</td>
</tr>
<tr>
<td>Step 7</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 8</td>
<td>errdisable recovery cause l2ptguard</td>
<td>(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.</td>
</tr>
<tr>
<td>Step 9</td>
<td>l2protocol-tunnel cos value</td>
<td>(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.</td>
</tr>
<tr>
<td>Step 10</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 11</td>
<td>show l2protocol</td>
<td>Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.</td>
</tr>
<tr>
<td>Step 12</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Use the `no l2protocol-tunnel [cdp | stp | vtp]` interface configuration command to disable protocol tunneling for one of the Layer 2 protocols or for all three. Use the `no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp]` and the `no l2protocol-tunnel drop-threshold [cdp | stp | vtp]` commands to return the shutdown and drop thresholds to the default settings.

This example shows how to configure Layer 2 protocol tunneling for CDP, STP, and VTP and to verify the configuration.

```
Switch(config)# interface fastethernet0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
```

**Configuring Layer 2 Tunneling for EtherChannels**

To configure Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels, you need to configure both the SP edge switch and the customer switch.

**Configuring the SP Edge Switch**

Beginning in privileged EXEC mode, follow these steps to configure a SP edge switch for Layer 2 protocol tunneling for EtherChannels:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and enter the interface to be configured as a tunnel port. This should be the edge port in the SP network that connects to the customer switch. Valid interfaces are physical interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode dot1q-tunnel</td>
<td>Configure the interface as an IEEE 802.1Q tunnel port.</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td><code>l2protocol-tunnel point-to-point</code> [pagp</td>
<td>lacp</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Caution</strong> To avoid a network failure, make sure that the network is a point-to-point topology before you enable tunneling for PAgP, LACP, or UDLD packets.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>l2protocol-tunnel shutdown-threshold</code> [point-to-point [pagp</td>
<td>lacp</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> If you also set a drop threshold on this interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>l2protocol-tunnel drop-threshold</code> [point-to-point [pagp</td>
<td>lacp</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> If you also set a shutdown threshold on this interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>no cdp enable</code></td>
<td>Disable CDP on the interface.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>spanning-tree bpdufilter enable</code></td>
<td>Enable BPDU filtering on the interface.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><code>errdisable recovery cause l2ptguard</code></td>
<td>(Optional) Configure the recovery mechanism from a Layer 2 maximum-rate error so that the interface is re-enabled and can try again. Errdisable recovery is disabled by default; when enabled, the default time interval is 300 seconds.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><code>l2protocol-tunnel cos</code> value</td>
<td>(Optional) Configure the CoS value for all tunneled Layer 2 PDUs. The range is 0 to 7; the default is the default CoS value for the interface. If none is configured, the default is 5.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><code>show l2protocol</code></td>
<td>Display the Layer 2 tunnel ports on the switch, including the protocols configured, the thresholds, and the counters.</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no l2protocol-tunnel [point-to-point [pagp | lacp | udld]]` interface configuration command to disable point-to-point protocol tunneling for one of the Layer 2 protocols or for all three. Use the `no l2protocol-tunnel shutdown-threshold [point-to-point [pagp | lacp | udld]]` and the `no l2protocol-tunnel drop-threshold [ [point-to-point [pagp | lacp | udld]]` commands to return the shutdown and drop thresholds to the default settings.
Chapter 16  Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling

Configuring the Customer Switch

After configuring the SP edge switch, begin in privileged EXEC mode and follow these steps to configure a customer switch for Layer 2 protocol tunneling for EtherChannels:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>switchport trunk encapsulation dot1q</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>switchport mode trunk</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>udld enable</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>channel-group channel-group-number mode desirable</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>interface port-channel port-channel number</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>shutdown</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>no shutdown</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>show l2protocol</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no switchport mode trunk, the no udld enable, and the no channel group channel-group-number mode desirable interface configuration commands to return the interface to the default settings.

For EtherChannels, you need to configure both the SP edge switches and the customer switches for Layer 2 protocol tunneling. (See Figure 16-6 on page 16-10.)

This example shows how to configure the SP edge switch 1 and edge switch 2. VLANs 17, 18, 19, and 20 are the access VLANs, Fast Ethernet interfaces 1 and 2 are point-to-point tunnel ports with PAgP and UDLD enabled, the drop threshold is 1000, and Fast Ethernet interface 3 is a trunk port.

SP edge switch 1 configuration:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
```
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk

SP edge switch 2 configuration:

Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport access vlan 19
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport access vlan 20
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/3
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk

This example shows how to configure the customer switch at Site 1. Fast Ethernet interfaces 1, 2, 3, and 4 are set for IEEE 802.1Q trunking, UDLD is enabled, EtherChannel group 1 is enabled, and the port channel is shut down and then enabled to activate the EtherChannel configuration.
Monitoring and Maintaining Tunneling Status

Table 16-2 shows the privileged EXEC commands for monitoring and maintaining IEEE 802.1Q and Layer 2 protocol tunneling.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear l2protocol-tunnel counters</td>
<td>Clear the protocol counters on Layer 2 protocol tunneling ports.</td>
</tr>
<tr>
<td>show dot1q-tunnel</td>
<td>Display IEEE 802.1Q tunnel ports on the switch.</td>
</tr>
<tr>
<td>show dot1q-tunnel interface interface-id</td>
<td>Verify if a specific interface is a tunnel port.</td>
</tr>
<tr>
<td>show l2protocol-tunnel</td>
<td>Display information about Layer 2 protocol tunneling ports.</td>
</tr>
<tr>
<td>show errdisable recovery</td>
<td>Verify if the recovery timer from a Layer 2 protocol-tunnel error disable state is enabled.</td>
</tr>
<tr>
<td>show l2protocol-tunnel interface interface-id</td>
<td>Display information about a specific Layer 2 protocol tunneling port.</td>
</tr>
<tr>
<td>show l2protocol-tunnel summary</td>
<td>Display only Layer 2 protocol summary information.</td>
</tr>
<tr>
<td>show vlan dot1q tag native</td>
<td>Display the status of native VLAN tagging on the switch.</td>
</tr>
</tbody>
</table>

For detailed information about these displays, see the command reference for this release.
Configuring STP

This chapter describes how to configure the Spanning Tree Protocol (STP) on port-based VLANs on the Catalyst 3560 switch. 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.

For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see Chapter 17, “Configuring MSTP.” For information about other spanning-tree features such as Port Fast, UplinkFast, root guard, and so forth, see Chapter 18, “Configuring Optional Spanning-Tree Features.”

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:
- Understanding Spanning-Tree Features, page 26-1
- Configuring Spanning-Tree Features, page 26-11
- Displaying the Spanning-Tree Status, page 26-22

Understanding Spanning-Tree Features

These sections contain this conceptual information:
- STP Overview, page 26-2
- Spanning-Tree Topology and BPDUs, page 26-3
- Bridge ID, Switch Priority, and Extended System ID, page 26-4
- Spanning-Tree Interface States, page 26-4
- How a Switch or Port Becomes the Root Switch or Root Port, page 26-7
- Spanning Tree and Redundant Connectivity, page 26-8
- Spanning-Tree Address Management, page 26-8
- Accelerated Aging to Retain Connectivity, page 26-8
- Spanning-Tree Modes and Protocols, page 26-9
- Supported Spanning-Tree Instances, page 26-9
STP Overview

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 port priority 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.

The default is for the switch to send keepalive messages (to ensure the connection is up) only on interfaces that do not have small form-factor pluggable (SFP) modules. You can use the `no keepalive` interface configuration command to change the default for an interface.
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).
  
  For each VLAN, the switch with the highest switch priority (the lowest numerical priority value) is elected as the root switch. If all switches are configured with the default priority (32768), the switch with the lowest MAC address in the VLAN becomes the root switch. The switch priority value occupies the most significant bits of the bridge ID, as shown in Table 26-1 on page 26-4.
- 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.

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.
Bridge ID, Switch 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 IDs 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. As shown in Table 26-1, 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 26-1 Switch Priority Value and Extended System ID

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

Spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN.

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. For more information, see the “Configuring the Root Switch” section on page 26-14, the “Configuring a Secondary Root Switch” section on page 26-16, and the “Configuring the Switch Priority of a VLAN” section on page 26-19.

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 26-1 illustrates how 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 the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the switch learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.
Blocking State

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

An interface in the blocking state performs these functions:
- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Listening State

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

An interface in the listening state performs these functions:
- Discards frames received on the interface
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Receives BPDUs

Learning State

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

An interface in the learning state performs these functions:
- Discards frames received on the interface
- 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
- Discards frames switched from another interface for forwarding
- Does not learn addresses
- Does not receive BPDUs

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

If all switches in a network are enabled with default spanning-tree settings, the switch with the lowest MAC address becomes the root switch. In Figure 26-2, 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.

![Figure 26-2 Spanning-Tree Topology](image)

<table>
<thead>
<tr>
<th>RP</th>
<th>DP</th>
<th>DP</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>A</td>
<td>D</td>
</tr>
<tr>
<td>DP</td>
<td>RP</td>
<td>DP</td>
</tr>
<tr>
<td>C</td>
<td>B</td>
<td>RP</td>
</tr>
<tr>
<td>DP</td>
<td>RP</td>
<td>DP</td>
</tr>
</tbody>
</table>

RP = Root Port
DP = Designated Port

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.
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, as shown in Figure 26-3. 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 lowest value.

![Figure 26-3 Spanning Tree and Redundant Connectivity](image)

You can also create redundant links between switches by using EtherChannel groups. For more information, see Chapter 35, “Configuring EtherChannels and Link-State Tracking.”

Spanning-Tree Address Management

IEEE 802.1D specifies 17 multicast addresses, ranging from 0x00180C200000 to 0x0180C2000010, to be used by different bridge protocols. These addresses are static addresses that cannot be removed. Regardless of the spanning-tree state, each switch receives but does not forward packets destined for addresses between 0x0180C2000000 and 0x0180C200000F.

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.

**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. It is the default spanning-tree mode used on all Ethernet port-based VLANs. 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 it uses a rapid convergence based on the IEEE 802.1w standard. 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.

  The 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 MSTP configuration and without having to reprovision 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. You cannot run MSTP without RSTP.

  The most common initial deployment of MSTP is in the backbone and distribution layers of a Layer 2 switched network. For more information, see Chapter 17, “Configuring MSTP.”

For information about the number of supported spanning-tree instances, see the next section.

**Supported Spanning-Tree Instances**

In PVST+ or rapid-PVST+ mode, the switch supports up to 128 spanning-tree instances.

In MSTP mode, the switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

For information about how spanning tree interoperates with the VLAN Trunking Protocol (VTP), see the “Spanning-Tree Configuration Guidelines” section on page 26-12.
Spanning-Tree Interoperability and Backward Compatibility

Table 26-2 lists the interoperability and compatibility among the supported spanning-tree modes in a network.

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

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.

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.

PVST+ is automatically enabled on IEEE 802.1Q trunks, and no user configuration is required. The external spanning-tree behavior on access ports and Inter-Switch Link (ISL) trunk ports is not affected by PVST+.

For more information on IEEE 802.1Q trunks, see Chapter 13, “Configuring VLANs.”

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 image installed on your switch. For more information, see Chapter 47, “Configuring Fallback Bridging.”

**Configuring Spanning-Tree Features**

These sections contain this configuration information:
- Default Spanning-Tree Configuration, page 26-11
- Spanning-Tree Configuration Guidelines, page 26-12
- Changing the Spanning-Tree Mode, page 26-13 (required)
- Disabling Spanning Tree, page 26-14 (optional)
- Configuring the Root Switch, page 26-14 (optional)
- Configuring a Secondary Root Switch, page 26-16 (optional)
- Configuring Port Priority, page 26-17 (optional)
- Configuring Path Cost, page 26-18 (optional)
- Configuring the Switch Priority of a VLAN, page 26-19 (optional)
- Configuring Spanning-Tree Timers, page 26-20 (optional)

**Default Spanning-Tree Configuration**

Table 26-3 shows the default spanning-tree configuration.

**Table 26-3 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. For more information, see the “Supported Spanning-Tree Instances” section on page 26-9.</td>
</tr>
<tr>
<td>Spanning-tree mode</td>
<td>PVST+. (Rapid 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. 100 Mb/s: 19. 10 Mb/s: 100.</td>
</tr>
<tr>
<td>Spanning-tree VLAN port priority (configurable on a per-VLAN basis)</td>
<td>128.</td>
</tr>
</tbody>
</table>
Spanning-Tree Configuration Guidelines

If more VLANs are defined in the VTP than there are spanning-tree instances, you can enable PVST+ or rapid PVST+ on only 128 VLANs on the switch. The remaining VLANs operate with spanning tree disabled. However, you can map multiple VLANs to the same spanning-tree instances by using MSTP. For more information, see Chapter 17, “Configuring MSTP.”

If 128 instances of spanning tree are already in use, you can disable spanning tree on one of the VLANs and then enable it on the VLAN where you want it to run. Use the `no spanning-tree vlan vlan-id` global configuration command to disable spanning tree on a specific VLAN, and use the `spanning-tree vlan vlan-id` global configuration command to enable spanning tree on the desired VLAN.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
</table>
| Spanning-tree VLAN port cost (configurable on a per-VLAN basis) | 1000 Mb/s: 4.  
100 Mb/s: 19.  
10 Mb/s: 100. |
| Spanning-tree timers                         | Hello time: 2 seconds.  
Forward-delay time: 15 seconds.  
Maximum-aging time: 20 seconds.  
Transmit hold count: 6 BPDUs |

Caution

Switches that are not running spanning tree still forward BPDUs that they receive so that the other switches on the VLAN that have a running spanning-tree instance can break loops. Therefore, spanning tree must be running on enough switches to break all the loops in the network; for example, at least one switch on each loop in the VLAN must be running spanning tree. It is not absolutely necessary to run spanning tree on all switches in the VLAN. However, if you are running spanning tree only on a minimal set of switches, an incautious change to the network that introduces another loop into the VLAN can result in a broadcast storm.

Note

If you have already used all available spanning-tree instances on your switch, adding another VLAN anywhere in the VTP domain creates a VLAN that is not running spanning tree on that switch. If you have the default allowed list on the trunk ports of that switch, 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 will not be broken, particularly if there are several adjacent switches that have all run out of spanning-tree instances. You can prevent this possibility by setting up allowed lists on the trunk ports of switches that have used up their allocation of spanning-tree instances. Setting up allowed lists is not necessary in many cases and can make it more labor-intensive to add another VLAN to the network.

Spanning-tree commands control the configuration of VLAN spanning-tree instances. You create a spanning-tree instance when you assign an interface to a VLAN. The spanning-tree instance is removed when the last interface is moved to another VLAN. You can configure switch and port parameters before a spanning-tree instance is created; these parameters are applied when the spanning-tree instance is created.
The switch supports PVST+, rapid PVST+, and MSTP, 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.) For information about the different spanning-tree modes and how they interoperate, see the “Spanning-Tree Interoperability and Backward Compatibility” section on page 26-10.

For configuration guidelines about UplinkFast and BackboneFast, see the “Optional Spanning-Tree Configuration Guidelines” section on page 18-10.

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.

Changing the Spanning-Tree Mode.

The switch supports three spanning-tree modes: PVST+, rapid PVST+, or MSTP. By default, the switch runs the PVST+ protocol.

Beginning in privileged EXEC mode, follow these steps to change the spanning-tree mode. If you want to enable a mode that is different from the default mode, this procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**spanning-tree mode { pvst</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><strong>Step 3</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>spanning-tree link-type point-to-point</strong></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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>clear spanning-tree detected-protocols</strong></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>
</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 specified in the “Supported Spanning-Tree Instances” section on page 26-9. 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.

Beginning in privileged EXEC mode, follow these steps to disable spanning-tree on a per-VLAN basis. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no spanning-tree vlan vlan-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree vlan vlan-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To re-enable spanning-tree, use the spanning-tree vlan vlan-id global configuration command.

Configuring the Root Switch

The switch maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the switch priority and the switch MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID becomes the root switch for that VLAN.

To configure a switch to become 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.
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 Table 26-1 on page 26-4.)

**Note**
The `spanning-tree vlan vlan-id root` global configuration command fails if the value necessary to be the root switch is less than 1.

**Note**
If your network consists of switches that both do 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.

**Note**
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 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.

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

Beginning in privileged EXEC mode, follow these steps to configure a switch to become the root for the specified VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>spanning-tree vlan vlan-id root primary</code> [diameter net-diameter [hello-time seconds]]</td>
<td>Configure a switch to become the root for the specified VLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>vlan-id</code>, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For <code>diameter net-diameter</code>, specify the maximum number of switches between any two end stations. The range is 2 to 7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For <code>hello-time seconds</code>, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To return to the default setting, use the **no spanning-tree vlan vlan-id root** global configuration command.

### Configuring a Secondary Root Switch

When you configure a switch 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 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.

Beginning in privileged EXEC mode, follow these steps to configure a switch to become the secondary root for the specified VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</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> spanning-tree vlan</td>
<td>Configure a switch to become the secondary root for the specified VLAN.</td>
</tr>
<tr>
<td>vlan-id root secondary [diameter</td>
<td>- For <code>vlan-id</code>, you can specify a single VLAN identified by VLAN</td>
</tr>
<tr>
<td>net-diameter [hello-time [seconds]]</td>
<td>ID number, a range of VLANs separated by a hyphen, or a series</td>
</tr>
<tr>
<td></td>
<td>of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <code>diameter net-diameter</code>, specify the maximum</td>
</tr>
<tr>
<td></td>
<td>number of switches between any two end stations. The range is</td>
</tr>
<tr>
<td></td>
<td>2 to 7.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <code>hello-time seconds</code>, specify the interval in</td>
</tr>
<tr>
<td></td>
<td>seconds between the generation of configuration messages by</td>
</tr>
<tr>
<td></td>
<td>the root switch. The range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td></td>
<td>Use the same network diameter and hello-time values that you used</td>
</tr>
<tr>
<td></td>
<td>when configuring the primary root switch. See the “Configuring</td>
</tr>
<tr>
<td></td>
<td>the Root Switch” section on page 26-14.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> show spanning-tree</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>detail</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> copy running-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no spanning-tree vlan vlan-id root** global configuration command.
Configuring Port Priority

If a loop occurs, spanning tree 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, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the port priority of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>spanning-tree port-priority priority</td>
</tr>
</tbody>
</table>
| Step 4  | spanning-tree vlan vlan-id port-priority priority | Configure 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. |
| Step 5  | end | Return to privileged EXEC mode. |
| Step 6  | show spanning-tree interface interface-id | Verify your entries. |
| Step 6  | show spanning-tree vlan vlan-id |  |
| Step 7  | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

**Note**

The show spanning-tree 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.
To return to the default setting, use the `no spanning-tree [vlan vlan-id] port-priority` interface configuration command. For information on how to configure load sharing on trunk ports by using spanning-tree port priorities, see the “Configuring Trunk Ports for Load Sharing” section on page 13-24.

## Configuring Path Cost

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.

Beginning in privileged EXEC mode, follow these steps to configure the cost of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical ports and port-channel logical interfaces (<code>port-channel port-channel-number</code>).</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>spanning-tree cost cost</code> Configure the cost for an interface. 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 <code>cost</code>, the range is 1 to 200000000; the default value is derived from the media speed of the interface.</td>
</tr>
</tbody>
</table>
| Step 4  | `spanning-tree vlan vlan-id cost cost` Configure the cost for a VLAN. 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.  
  - For `cost`, the range is 1 to 200000000; the default value is derived from the media speed of the interface. |
| Step 5  | `end` Return to privileged EXEC mode. |
| Step 6  | `show spanning-tree interface interface-id` or `show spanning-tree vlan vlan-id` Verify your entries. |
| Step 7  | `copy running-config startup-config` (Optional) Save your entries in the configuration file. |
To return to the default setting, use the no spanning-tree [vlan vlan-id] cost interface configuration command. For information on how to configure load sharing on trunk ports by using spanning-tree path costs, see the “Configuring Trunk Ports for Load Sharing” section on page 13-24.

## Configuring the Switch Priority of a VLAN

You can configure the switch priority and make it more likely that the 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.

Beginning in privileged EXEC mode, follow these steps to configure the switch priority of a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>spanning-tree vlan vlan-id priority priority</td>
<td>Configure the switch priority of a VLAN.</td>
</tr>
<tr>
<td></td>
<td>• For vlan-id, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show spanning-tree vlan vlan-id</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no spanning-tree vlan vlan-id priority global configuration command.
Configuring Spanning-Tree Timers

Table 26-4 describes the timers that affect the entire spanning-tree performance.

Table 26-4  Spanning-Tree Timers

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello timer</td>
<td>Controls how often the switch broadcasts hello messages to other switches.</td>
</tr>
<tr>
<td>Forward-delay timer</td>
<td>Controls how long each of the listening and learning states last before the interface begins forwarding.</td>
</tr>
<tr>
<td>Maximum-age timer</td>
<td>Controls the amount of time the switch stores protocol information received on an interface.</td>
</tr>
<tr>
<td>Transmit hold count</td>
<td>Controls the number of BPDUs that can be sent before pausing for 1 second.</td>
</tr>
</tbody>
</table>

The sections that follow provide the configuration steps.

Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

**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 hello time.

Beginning in privileged EXEC mode, follow these steps to configure the hello time of a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2    | `spanning-tree vlan vlan-id hello-time seconds` | Configure the hello time of a VLAN. The hello time is the interval between the generation of configuration messages 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. |
| Step 3    | `end`                                | Return to privileged EXEC mode.                                         |
| Step 4    | `show spanning-tree vlan vlan-id`   | Verify your entries.                                                    |
| Step 5    | `copy running-config startup-config` | (Optional) Save your entries in the configuration file.                 |

To return to the default setting, use the `no spanning-tree vlan vlan-id hello-time` global configuration command.
Configuring the Forwarding-Delay Time for a VLAN

Beginning in privileged EXEC mode, follow these steps to configure the forwarding-delay time for a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree vlan vlan-id forward-time seconds</td>
<td>Configure the forward time of a VLAN. The forward 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></td>
<td>• For <code>vlan-id</code>, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For <code>seconds</code>, the range is 4 to 30; the default is 15.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree vlan vlan-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no spanning-tree vlan vlan-id forward-time` global configuration command.

Configuring the Maximum-Aging Time for a VLAN

Beginning in privileged EXEC mode, follow these steps to configure the maximum-aging time for a VLAN. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree vlan vlan-id max-age seconds</td>
<td>Configure 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>• For <code>vlan-id</code>, you can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For <code>seconds</code>, the range is 6 to 40; the default is 20.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree vlan vlan-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no spanning-tree vlan vlan-id max-age` global configuration command.
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.

Beginning in privileged EXEC mode, follow these steps to configure the transmit hold-count. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree transmit hold-count value</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree detail</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no spanning-tree transmit hold-count value global configuration command.

Displaying the Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 26-5:

<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 summary [totals]</td>
<td>Displays a summary of interface states or displays the total lines of the STP state section.</td>
</tr>
</tbody>
</table>

You can clear spanning-tree counters by using the clear spanning-tree [interface interface-id] privileged EXEC command.

For information about other keywords for the show spanning-tree privileged EXEC command, see the command reference for this release.
Configuring MSTP

This chapter describes how to configure the Cisco implementation of the IEEE 802.1s Multiple STP (MSTP) on the Catalyst 3560 switch.

Note

The multiple spanning-tree (MST) implementation is based on the IEEE 802.1s standard. The MST implementations in Cisco IOS releases earlier than Cisco IOS Release 12.2(25)SECare prestandard.

The MSTP enables multiple VLANs to be 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 and enables load balancing. It improves the fault tolerance of the network because a failure in one instance (forwarding path) does not affect other instances (forwarding paths). 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 Rapid Spanning Tree Protocol (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 per-VLAN spanning-tree plus (PVST+) and rapid per-VLAN spanning-tree plus (rapid PVST+). For information about PVST+ and rapid PVST+, see Chapter 26, “Configuring STP.” For information about other spanning-tree features such as Port Fast, UplinkFast, root guard, and so forth, see Chapter 18, “Configuring Optional Spanning-Tree Features.”

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding MSTP, page 17-2
- Understanding RSTP, page 17-9
- Configuring MSTP Features, page 17-14
- Displaying the MST Configuration and Status, page 17-27
Understanding MSTP

MSTP, which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides 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.

These sections describe how the MSTP works:

- Multiple Spanning-Tree Regions, page 17-2
- IST, CIST, and CST, page 17-2
- Hop Count, page 17-6
- Boundary Ports, page 17-6
- IEEE 802.1s Implementation, page 17-7
- Interoperability with IEEE 802.1D STP, page 17-8

For configuration information, see the “Configuring MSTP Features” section on page 17-14.

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 as shown in Figure 17-1 on page 17-4.

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 using the `spanning-tree mst configuration` global configuration command, after which the switch enters the MST configuration mode. From this mode, you can map VLANs to an MST instance by using the `instance` MST configuration command, specify the region name by using the `name` MST configuration command, and set the revision number by using the `revision` MST configuration command.

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.

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.

For more information, see the “Operations Within an MST Region” section on page 17-3 and the “Operations Between MST Regions” section on page 17-3.

Note

The implementation of the IEEE 802.1s standard, changes some of the terminology associated with MST implementations. For a summary of these changes, see Table 26-1 on page 26-4.

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) as shown in Figure 17-1 on page 17-4. 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. Thus 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.

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.

Figure 17-1 shows a network with 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.

*Figure 17-1  MST Regions, CIST Masters, and CST Root*
Only the CST instance sends and receives BPDUs, and MST instances add their spanning-tree information into the BPDUs to interact with neighboring switches and compute the final spanning-tree topology. Because of this, the spanning-tree parameters related to BPDU transmission (for example, hello time, forward time, max-age, and max-hops) are configured only on the CST instance but affect all MST instances. Parameters related to the spanning-tree topology (for example, switch priority, port VLAN cost, and port VLAN priority) can be configured on both the CST instance and the MST instance.

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

### 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.

- **CIST root** is the root switch for the unique instance that spans the whole network, the CIST.
- **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.
- **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.
- **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 17-1 on page 17-5 compares the IEEE standard and the Cisco prestandard 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>
Hop Count

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

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

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

Boundary Ports

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

There is no definition of a boundary port in the IEEE 802.1s standard. The IEEE 802.1Q-2002 standard identifies two kinds of messages that a port can receive: internal (coming from the same region) and external. 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. When a message is internal, the CIST part is received by the CIST, and each MST instance receives its respective M-record. The Cisco prestandard implementation treats a port that receives an external message as a boundary port. This means a port cannot receive a mix of internal and external messages.

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 receiving both internal and external messages on a port.

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.

---

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

The other change from the 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 cases exist now:

- 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 BPDU. 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 17-2 illustrates this scenario. 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 thus 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 BPDU. The port BY is thus 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.
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 discarding state because disrupting connectivity in case of inconsistency is preferable to opening a bridging loop.

**Figure 17-3** 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, thus preventing 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.

**Understanding RSTP**

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).

These sections describe how the RSTP works:

- Port Roles and the Active Topology, page 17-9
- Rapid Convergence, page 17-10
- Synchronization of Port Roles, page 17-11
- Bridge Protocol Data Unit Format and Processing, page 17-12

For configuration information, see the “Configuring MSTP Features” section on page 17-14.

**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 as described in the “Spanning-Tree Topology and BPDUs” section on page 26-3. Then the RSTP 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 17-2 provides a comparison of IEEE 802.1D and RSTP port states.

Table 17-2 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.

As shown in Figure 17-4, 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.

**Figure 17-4 Proposal and Agreement Handshaking for Rapid Convergence**

![Diagram of Proposal and Agreement Handshaking for Rapid Convergence]

**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.
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. The sequence of events is shown in Figure 17-5.

**Figure 17-5 Sequence of Events During Rapid Convergence**

The sequence of events is shown in Figure 17-5.

---

**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 17-3 shows the RSTP flag fields.

**Table 17-3 RSTP BPDU Flags**

<table>
<thead>
<tr>
<th>Bit</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Topology change (TC)</td>
</tr>
<tr>
<td>1</td>
<td>Proposal</td>
</tr>
<tr>
<td>2–3:</td>
<td>Port role:</td>
</tr>
<tr>
<td>00</td>
<td>Unknown</td>
</tr>
<tr>
<td>01</td>
<td>Alternate port</td>
</tr>
<tr>
<td>10</td>
<td>Root port</td>
</tr>
<tr>
<td>11</td>
<td>Designated port</td>
</tr>
<tr>
<td>4</td>
<td>Learning</td>
</tr>
<tr>
<td>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 (higher switch ID, higher path cost, and so forth 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.

Configuring MSTP Features

These sections contain this configuration information:

• Default MSTP Configuration, page 17-15
• MSTP Configuration Guidelines, page 17-15
• Specifying the MST Region Configuration and Enabling MSTP, page 17-16 (required)
• Configuring the Root Switch, page 17-18 (optional)
• Configuring a Secondary Root Switch, page 17-19 (optional)
• Configuring Port Priority, page 17-20 (optional)
• Configuring Path Cost, page 17-21 (optional)
• Configuring the Switch Priority, page 17-23 (optional)
• Configuring the Hello Time, page 17-24 (optional)
• Configuring the Forwarding-Delay Time, page 17-24 (optional)
• Configuring the Maximum-Aging Time, page 17-25 (optional)
• Configuring the Maximum-Hop Count, page 17-25 (optional)
• Specifying the Link Type to Ensure Rapid Transitions, page 17-26 (optional)
• Designating the Neighbor Type, page 17-26 (optional)
• Restarting the Protocol Migration Process, page 17-27 (optional)
Default MSTP Configuration

Table 17-4 shows the default MSTP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning-tree mode</td>
<td>PVST+ (Rapid PVST+ and MSTP are disabled).</td>
</tr>
<tr>
<td>Switch priority (configurable on a per-CIST port basis)</td>
<td>32768.</td>
</tr>
<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>1000 Mbps: 4.</td>
</tr>
<tr>
<td></td>
<td>100 Mbps: 19.</td>
</tr>
<tr>
<td></td>
<td>10 Mbps: 100.</td>
</tr>
<tr>
<td>Hello time</td>
<td>2 seconds.</td>
</tr>
<tr>
<td>Forward-delay time</td>
<td>15 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>

For information about the supported number of spanning-tree instances, see the “Supported Spanning-Tree Instances” section on page 26-9.

MSTP Configuration Guidelines

These are the configuration guidelines for MSTP:

- When you enable MST by using the `spanning-tree mode mst` global configuration command, RSTP is automatically enabled.
- For two or more switches to be in the same MST region, they must have the same VLAN-to-instance map, the same configuration revision number, and the same name.
- The switch supports up to 65 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.
- 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.) For more information, see the “Spanning-Tree Interoperability and Backward Compatibility” section on page 26-10. For information on the recommended trunk port configuration, see the “Interaction with Other Features” section on page 13-19.
- 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 SNMP support.
- 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.
- All MST boundary ports must be forwarding for load balancing between a PVST+ and an MST cloud or between a rapid-PVST+ and an MST cloud. For this to occur, the IST master of the MST cloud should also be the root of the CST. If the MST cloud consists of multiple MST regions, one
Configuring MSTP Features

Chapter 17 Configuring MSTP

Configuring MSTP Features

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.

- 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.

- For configuration guidelines about, see the “Optional Spanning-Tree Configuration Guidelines” section on page 18-10.

- 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, these 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>

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.

Beginning in privileged EXEC mode, follow these steps to specify the MST region configuration and enable MSTP. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree mst configuration</td>
<td>Enter MST configuration mode.</td>
</tr>
<tr>
<td>Step 3 instance instance-id vlan vlan-range</td>
<td>Map VLANs to an MST instance.</td>
</tr>
<tr>
<td></td>
<td>• For instance-id, the range is 0 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• For vlan vlan-range, the range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td>When you map VLANs to an MST instance, the mapping</td>
</tr>
<tr>
<td></td>
<td>is incremental, and the VLANs specified in the</td>
</tr>
<tr>
<td></td>
<td>command are added to or removed from the VLANs that</td>
</tr>
<tr>
<td></td>
<td>were previously mapped.</td>
</tr>
<tr>
<td></td>
<td>To specify a VLAN range, use a hyphen; for example,</td>
</tr>
<tr>
<td></td>
<td>instance 1 vlan 1-63 maps VLANs 1 through 63 to MST</td>
</tr>
<tr>
<td></td>
<td>instance 1.</td>
</tr>
<tr>
<td></td>
<td>To specify a VLAN series, use a comma; for example,</td>
</tr>
<tr>
<td></td>
<td>instance 1 vlan 10, 20, 30 maps VLANs 10, 20, and</td>
</tr>
<tr>
<td></td>
<td>30 to MST instance 1.</td>
</tr>
</tbody>
</table>
To return to the default MST region configuration, use the `no spanning-tree mst configuration` global configuration command. To return to the default VLAN-to-instance map, use the `no instance instance-id [vlan vlan-range]` MST configuration command. To return to the default name, use the `no name MST` configuration command. To return to the default revision number, use the `no revision MST` configuration command. To re-enable PVST+, use the `no spanning-tree mode` or the `spanning-tree mode pvst` global configuration command.

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region `region1`, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name  [region1]
Revision 1
```
Configuring MSTP Features

<table>
<thead>
<tr>
<th>Instance</th>
<th>Vlans Mapped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1-9, 21-4094</td>
</tr>
<tr>
<td>1</td>
<td>10-20</td>
</tr>
</tbody>
</table>

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

Configuring the 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.

To configure a switch to become the root, use the `spanning-tree mst instance-id root` global configuration command to 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 switch 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 as shown in Table 26-1 on page 26-4.)

If your network consists of switches that both do 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.

**Note**

After configuring the switch as the root switch, we recommend that you avoid manually configuring the hello time, forward-delay time, and maximum-age time through the `spanning-tree mst hello-time`, `spanning-tree mst forward-time`, and the `spanning-tree mst max-age` global configuration commands.
Beginning in privileged EXEC mode, follow these steps to configure a switch as the root switch. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>spanning-tree mst instance-id root primary [diameter net-diameter [hello-time seconds]]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show spanning-tree mst instance-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the no spanning-tree mst instance-id root global configuration command.

### 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.
Chapter 17  Configuring MSTP

Configuring MSTP Features

Beginning in privileged EXEC mode, follow these steps to configure a switch as the secondary root switch. This procedure is optional.

### 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.

Beginning in privileged EXEC mode, follow these steps to configure the MSTP port priority of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree mst instance-id root secondary [diameter net-diameter [hello-time seconds]]</td>
<td>Configure a switch as the secondary root switch.</td>
</tr>
<tr>
<td></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>• (Optional) For diameter net-diameter, specify the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For hello-time seconds, specify the interval in seconds between the generation of configuration messages by the root switch. The range is 1 to 10 seconds; the default is 2 seconds.</td>
</tr>
<tr>
<td></td>
<td>Use the same network diameter and hello-time values that you used when configuring the primary root switch. See the “Configuring the Root Switch” section on page 17-18.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree mst instance-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the **no spanning-tree mst instance-id root** global configuration command.

### Command Purpose

| Step 1 configure terminal                    | Enter global configuration mode.                                        |
| Step 2 interface interface-id               | Specify an interface to configure, and enter interface configuration mode. |
|                                               | Valid interfaces include physical ports and port-channel logical interfaces. The port-channel range is 1 to 48. |
Configuring MSTP Features

### 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.

Beginning in privileged EXEC mode, follow these steps to configure the MSTP cost of an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical ports and port-channel logical interfaces. The port-channel range is 1 to 48.</td>
</tr>
</tbody>
</table>
### Configuring MSTP Features

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>spanning-tree mst instance-id cost cost</code></td>
<td>Configure 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></td>
<td></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></td>
<td></td>
<td>- For <code>cost</code>, the range is 1 to 200000000; the default value is derived from the media speed of the interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show spanning-tree mst interface interface-id</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>or <code>show spanning-tree mst instance-id</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Note

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.

To return the interface to its default setting, use the `no spanning-tree mst instance-id cost` interface configuration command.
Configuring the Switch Priority

You can configure the switch priority and make it more likely that the 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 mst instance-id root primary` and the `spanning-tree mst instance-id root secondary` global configuration commands to modify the switch priority.

Beginning in privileged EXEC mode, follow these steps to configure the switch priority. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree mst instance-id priority priority</td>
</tr>
<tr>
<td></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></td>
<td>• For <code>priority</code>, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch.</td>
</tr>
<tr>
<td></td>
<td>Priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show spanning-tree mst instance-id</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no spanning-tree mst instance-id priority` global configuration command.
Configuring the Hello Time

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

Beginning in privileged EXEC mode, follow these steps to configure the hello time for all MST instances. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree mst hello-time seconds</td>
<td>Configure the hello time for all MST instances. The hello time is the interval between the generation of configuration messages by the root switch. These messages mean that the switch is alive. For seconds, the range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree mst</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the no spanning-tree mst hello-time global configuration command.

Configuring the Forwarding-Delay Time

Beginning in privileged EXEC mode, follow these steps to configure the forwarding-delay time for all MST instances. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 spanning-tree mst forward-time seconds</td>
<td>Configure the forward time for all MST instances. The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state. For seconds, the range is 4 to 30; the default is 15.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show spanning-tree mst</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the no spanning-tree mst forward-time global configuration command.
Configuring the Maximum-Aging Time

Beginning in privileged EXEC mode, follow these steps to configure the maximum-ageing time for all MST instances. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree mst max-age <em>seconds</em></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show spanning-tree mst</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no spanning-tree mst max-age` global configuration command.

Configuring the Maximum-Hop Count

Beginning in privileged EXEC mode, follow these steps to configure the maximum-hop count for all MST instances. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree mst max-hops <em>hop-count</em></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show spanning-tree mst</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return the switch to its default setting, use the `no spanning-tree mst max-hops` global configuration command.
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 as described in the “Rapid Convergence” section on page 17-10.

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.

Beginning in privileged EXEC mode, follow these steps to override the default link-type setting. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify an interface to configure, and enter 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>
<tr>
<td>spanning-tree link-type point-to-point</td>
<td>Specify that the link type of a port is point-to-point.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show spanning-tree mst interface interface-id</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the port to its default setting, use the no spanning-tree link-type interface configuration command.

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.

Beginning in privileged EXEC mode, follow these steps to override the default link-type setting. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify an interface to configure, and enter interface configuration mode. Valid interfaces include physical ports.</td>
</tr>
<tr>
<td>spanning-tree mst pre-standard</td>
<td>Specify that the port can send only prestandard BPDUs.</td>
</tr>
</tbody>
</table>
To return the port to its default setting, use the `no spanning-tree mst prestandard` interface configuration command.

**Restarting the 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.

To restart the protocol migration process (force the renegotiation with neighboring switches) on the switch, use the `clear spanning-tree detected-protocols` privileged EXEC command.

To restart the protocol migration process on a specific interface, use the `clear spanning-tree detected-protocols interface interface-id` privileged EXEC command.

**Displaying the MST Configuration and Status**

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 17-5:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show spanning-tree mst configuration</code></td>
<td>Displays the MST region configuration.</td>
</tr>
<tr>
<td><code>show spanning-tree mst configuration digest</code></td>
<td>Displays the MD5 digest included in the current MSTCI.</td>
</tr>
<tr>
<td><code>show spanning-tree mst instance-id</code></td>
<td>Displays MST information for the specified instance.</td>
</tr>
<tr>
<td><code>show spanning-tree mst interface interface-id</code></td>
<td>Displays MST information for the specified interface.</td>
</tr>
</tbody>
</table>

For information about other keywords for the `show spanning-tree` privileged EXEC command, see the command reference for this release.
Configuring Optional Spanning-Tree Features

This chapter describes how to configure optional spanning-tree features on the Catalyst 3560 switch. You can configure all of these features when your switch is running the per-VLAN spanning-tree plus (PVST+). You can configure only the noted features when your switch is running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol.

For information on configuring the PVST+ and rapid PVST+, see Chapter 26, “Configuring STP.” For information about the Multiple Spanning Tree Protocol (MSTP) and how to map multiple VLANs to the same spanning-tree instance, see Chapter 17, “Configuring MSTP.”

This chapter consists of these sections:

- Understanding Optional Spanning-Tree Features, page 18-1
- Configuring Optional Spanning-Tree Features, page 18-10
- Displaying the Spanning-Tree Status, page 18-17

Understanding Optional Spanning-Tree Features

These sections contain this conceptual information:

- Understanding Port Fast, page 18-2
- Understanding BPDU Guard, page 18-2
- Understanding BPDU Filtering, page 18-3
- Understanding UplinkFast, page 18-3
- Understanding BackboneFast, page 18-5
- Understanding EtherChannel Guard, page 18-7

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.
Understanding Port Fast

Port Fast 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. You can use Port Fast on interfaces connected to a single workstation or server, as shown in Figure 18-1, 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 Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

**Note**

Because the purpose of Port Fast is to minimize the time interfaces must wait for spanning-tree to converge, it is effective only when used on interfaces connected to end stations. If you enable Port Fast on an interface connecting to another switch, you risk creating a spanning-tree loop.

You can enable this feature by using the `spanning-tree portfast` interface configuration or the `spanning-tree portfast default` global configuration command.

![Figure 18-1 Port Fast-Enabled Interfaces](image)

Understanding BPDU Guard

The BPDU guard feature can be globally enabled on the switch or can be enabled per port, but the feature operates with some differences.

At the global level, you enable BPDU guard on Port Fast-enabled ports by using the `spanning-tree portfast bpduguard default` global configuration command. Spanning tree shuts down ports that are in a Port Fast-operational state if any BPDU is received on them. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-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.

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.

At the interface level, you enable BPDU guard on any port by using the `spanning-tree bpduguard enable` interface configuration command without also enabling the Port Fast feature. When 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.

**Understanding 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.

At the global level, you can enable BPDU filtering on Port Fast-enabled interfaces by using the `spanning-tree portfast bpdufilter default` global configuration command. This command prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

At the interface level, you can enable BPDU filtering on any interface by using the `spanning-tree bpdufilter enable` interface configuration command without also enabling the Port Fast 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 for the entire switch or for an interface.

**Understanding UplinkFast**

Switches in hierarchical networks can be grouped into backbone switches, distribution switches, and access switches. Figure 18-2 shows a complex network where distribution switches and access switches each have at least one redundant link that spanning tree blocks to prevent loops.
Understanding Optional Spanning-Tree Features

If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the `spanning-tree uplinkfast` global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures.

When the spanning tree reconfigures the new root port, other interfaces flood the network with multicast packets, one for each address that was learned on the interface. You can limit these bursts of multicast traffic by reducing the `max-update-rate` parameter (the default for this parameter is 150 packets per second). However, if you enter zero, station-learning frames are not generated, so the spanning-tree topology converges more slowly after a loss of connectivity.

**Note**

UplinkFast is most useful in wiring-closet switches at the access or edge of the network. It is not appropriate for backbone devices. This feature might not be useful for other types of applications.

UplinkFast provides fast convergence after a direct link failure and achieves load balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 interfaces (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.

**Figure 18-3** shows an example topology with no link failures. Switch A, the root switch, is connected directly to Switch B over link L1 and to Switch C over link L2. The Layer 2 interface on Switch C that is connected directly to Switch B is in a blocking state.
Figure 18-3  UplinkFast Example Before Direct Link Failure

If Switch C detects a link failure on the currently active link L2 on the root port (a direct link failure), UplinkFast unblocks the blocked interface on Switch C and transitions it to the forwarding state without going through the listening and learning states, as shown in Figure 18-4. This change takes approximately 1 to 5 seconds.

Figure 18-4  UplinkFast Example After Direct Link Failure

Understanding 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, which is enabled by using the `spanning-tree backbonefast` global configuration command, starts when a root port or blocked interface on a switch receives inferior BPDUs from its designated switch. An inferior BPDU identifies a switch that declares itself as both the root bridge and the designated switch. When a switch receives an inferior BPDU, it means that a link to which the switch is not directly connected (an indirect link) has failed (that is, the designated switch has lost its connection to the root switch). Under spanning-tree rules, the switch ignores inferior BPDUs for the configured maximum aging time specified by the `spanning-tree vlan vlan-id max-age` global configuration command.
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 has alternate paths to the root switch, it uses these alternate paths to send a root link query (RLQ) request. The switch sends the RLQ request on all alternate paths and waits for an RLQ reply from other switches in the network.

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 18-5 shows 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.

If link L1 fails as shown in Figure 18-6, 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 BPDUs to Switch C, identifying itself as the root. When Switch C receives the inferior BPDUs 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. Figure 18-6 shows how BackboneFast reconfigures the topology to account for the failure of link L1.
If a new switch is introduced into a shared-medium topology as shown in Figure 18-7, 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.

**Figure 18-7 Adding a Switch in a Shared-Medium Topology**

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. For EtherChannel configuration guidelines, see the “EtherChannel Configuration Guidelines” section on page 35-10.

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.

You can enable this feature by using the `spanning-tree etherchannel guard misconfig` global configuration command.
Understanding Root Guard

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, as shown in Figure 18-8. 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.

You can enable this feature by using the spanning-tree guard root interface configuration command.

Caution

Misuse of the root-guard feature can cause a loss of connectivity.

Figure 18-8  Root Guard in a Service-Provider Network

Enable the root-guard feature on these interfaces to prevent switches in the customer network from becoming the root switch or being in the path to the root.
Understanding 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.

You can enable this feature by using the `spanning-tree loopguard default` global configuration command.

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.
Configuring Optional Spanning-Tree Features

These sections contain this configuration information:

- Default Optional Spanning-Tree Configuration, page 18-10
- Optional Spanning-Tree Configuration Guidelines, page 18-10
- Enabling Port Fast, page 18-10 (optional)
- Enabling BPDU Guard, page 18-12 (optional)
- Enabling BPDU Filtering, page 18-13 (optional)
- Enabling UplinkFast for Use with Redundant Links, page 18-14 (optional)
- Enabling BackboneFast, page 18-14 (optional)
- Enabling EtherChannel Guard, page 18-15 (optional)
- Enabling Root Guard, page 18-16 (optional)
- Enabling Loop Guard, page 18-16 (optional)

Default Optional Spanning-Tree Configuration

Table 18-1 shows the default optional spanning-tree configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Fast, BPDU filtering, BPDU guard</td>
<td>Globally disabled (unless they are individually configured per interface).</td>
</tr>
<tr>
<td>UplinkFast</td>
<td>Globally disabled.</td>
</tr>
<tr>
<td>BackboneFast</td>
<td>Globally disabled.</td>
</tr>
<tr>
<td>EtherChannel guard</td>
<td>Globally enabled.</td>
</tr>
<tr>
<td>Root guard</td>
<td>Disabled on all interfaces.</td>
</tr>
<tr>
<td>Loop guard</td>
<td>Disabled on all interfaces.</td>
</tr>
</tbody>
</table>

Optional Spanning-Tree Configuration Guidelines

You can configure PortFast, BPDU guard, BPDU filtering, EtherChannel guard, root guard, or loop guard if your switch is running PVST+, rapid PVST+, or MSTP.

You can configure the UplinkFast or 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+.

Enabling Port Fast

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting for the standard forward-time delay.
Use Port Fast 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.

If you enable the voice VLAN feature, the Port Fast feature is automatically enabled. When you disable voice VLAN, the Port Fast feature is not automatically disabled. For more information, see Chapter 12, “Configuring Voice VLAN.”

You can enable this feature if your switch is running PVST+, rapid PVST+, or MSTP.

Beginning in privileged EXEC mode, follow these steps to enable Port Fast. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>spanning-tree portfast [trunk]</td>
</tr>
</tbody>
</table>

**Note** To enable Port Fast on trunk ports, you must use the spanning-tree portfast trunk interface configuration command. The spanning-tree portfast command will not work on trunk ports.

**Caution** Make sure that there are no loops in the network between the trunk port and the workstation or server before you enable Port Fast on a trunk port.

By default, Port Fast is disabled on all interfaces.

| Step 4 | end | Return to privileged EXEC mode. |
| Step 5 | show spanning-tree interface interface-id portfast | Verify your entries. |
| Step 6 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

**Note** You can use the spanning-tree portfast default global configuration command to globally enable the Port Fast feature on all nontrunking ports.

To disable the Port Fast feature, use the spanning-tree portfast disable interface configuration command.
Enabling BPDU Guard

When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree continues to run on the ports. They remain up unless they receive a BPDU.

In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-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.

To prevent the port from shutting down, you can use the `errdisable detect cause bpdu guard shutdown vlan` global configuration command to shut down just the offending VLAN on the port where the violation occurred.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

Caution

Configure Port Fast 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.

You also can use the `spanning-tree bpdu guard enable` interface configuration command to enable BPDU guard on any port without also enabling the Port Fast feature. When the port receives a BPDU, it is put in the error-disabled state.

You can enable the BPDU guard feature if your switch is running PVST+, rapid PVST+, or MSTP. Beginning in privileged EXEC mode, follow these steps to globally enable the BPDU guard feature. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>spanning-tree portfast bpdu guard default</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>spanning-tree portfast</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable BPDU guard, use the `no spanning-tree portfast bpdu guard default` global configuration command.

You can override the setting of the `no spanning-tree portfast bpdu guard default` global configuration command by using the `spanning-tree bpdu guard enable` interface configuration command.
Enabling BPDU Filtering

When you globally enable BPDU filtering on Port Fast-enabled interfaces, it prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

⚠️ Caution
Configure Port Fast 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.

You can also use the `spanning-tree bpdufilter enable` interface configuration command to enable BPDU filtering on any interface without also enabling the Port Fast 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.

Beginning in privileged EXEC mode, follow these steps to globally enable the BPDU filtering feature. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>spanning-tree portfast bpdufilter default</td>
<td>Globally enable BPDU filtering. By default, BPDU filtering is disabled.</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
<td>Specify the interface connected to an end station, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>spanning-tree portfast</td>
<td>Enable the Port Fast feature.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable BPDU filtering, use the `no spanning-tree portfast bpdufilter default` global configuration command.

You can override the setting of the `no spanning-tree portfast bpdufilter default` global configuration command by using the `spanning-tree bpdufilter enable` interface configuration command.
Enabling UplinkFast for Use with Redundant Links

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 by using the `no spanning-tree vlan vlan-id priority` global configuration command.

**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+.

Beginning in privileged EXEC mode, follow these steps to enable UplinkFast. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>(Optional) For <code>pkts-per-second</code>, the range is 0 to 32000 packets per second; the default is 150.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show spanning-tree summary</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

When UplinkFast is enabled, the switch priority of all VLANs is set to 49152. If you change the path cost to a value less than 3000 and you enable UplinkFast or UplinkFast is already enabled, the path cost of all interfaces and VLAN trunks is increased by 3000 (if you change the path cost to 3000 or above, the path cost is not altered). The changes to the switch priority and the path cost reduce the chance that a switch will become the root switch.

When UplinkFast is disabled, the switch priorities of all VLANs and path costs of all interfaces are set to default values if you did not modify them from their defaults.

To return the update packet rate to the default setting, use the `no spanning-tree uplinkfast max-update-rate` global configuration command. To disable UplinkFast, use the `no spanning-tree uplinkfast` command.

Enabling BackboneFast

You can enable BackboneFast to detect indirect link failures and to start the spanning-tree reconfiguration sooner.

**Note**
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.
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+.

Beginning in privileged EXEC mode, follow these steps to enable BackboneFast. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>spanning-tree backbonefast</td>
<td>Enable BackboneFast.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show spanning-tree summary</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the BackboneFast feature, use the `no spanning-tree backbonefast` global configuration command.

### Enabling EtherChannel Guard

You can enable EtherChannel guard to detect an EtherChannel misconfiguration if your switch is running PVST+, rapid PVST+, or MSTP.

Beginning in privileged EXEC mode, follow these steps to enable EtherChannel guard. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>spanning-tree etherchannel guard</td>
<td>Enable EtherChannel guard.</td>
</tr>
<tr>
<td>misconfig</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show spanning-tree summary</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the EtherChannel guard feature, use the `no spanning-tree etherchannel guard misconfig` global configuration command.

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.
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.

Beginning in privileged EXEC mode, follow these steps to enable root guard on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>spanning-tree guard root</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable root guard, use the no spanning-tree guard interface configuration command.

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.

Beginning in privileged EXEC mode, follow these steps to enable loop guard. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>show spanning-tree active or show spanning-tree mst</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
To globally disable loop guard, use the `no spanning-tree loopguard default` global configuration command. You can override the setting of the `no spanning-tree loopguard default` global configuration command by using the `spanning-tree guard loop` interface configuration command.

### Displaying the Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 18-2:

<table>
<thead>
<tr>
<th>Command</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 interface interface-id</code></td>
<td>Displays spanning-tree information for the specified interface.</td>
</tr>
<tr>
<td><code>show spanning-tree mst interface interface-id</code></td>
<td>Displays MST information for the specified interface.</td>
</tr>
<tr>
<td><code>show spanning-tree summary</code></td>
<td>Displays a summary of interface states or displays the total lines of the spanning-tree state section.</td>
</tr>
</tbody>
</table>

You can clear spanning-tree counters by using the `clear spanning-tree [interface interface-id]` privileged EXEC command.

For information about other keywords for the `show spanning-tree` privileged EXEC command, see the command reference for this release.
Configuring Flex Links and the MAC Address-Table Move Update Feature

This chapter describes how to configure Flex Links, a pair of interfaces on the Catalyst 3560 switch that provide a mutual backup. It also describes how to configure the MAC address-table move update feature, also referred to as the Flex Links bidirectional fast convergence feature.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

The chapter consists of these sections:
- Understanding Flex Links and the MAC Address-Table Move Update, page 19-1
- Configuring Flex Links and the MAC Address-Table Move Update, page 19-7
- Monitoring Flex Links and the MAC Address-Table Move Update, page 19-14

Understanding Flex Links and the MAC Address-Table Move Update

This section contains this information:
- Flex Links, page 19-1
- VLAN Flex Link Load Balancing and Support, page 19-3
- Flex Link Multicast Fast Convergence, page 19-3
- MAC Address-Table Move Update, page 19-6

Flex Links

Flex Links are a pair of a Layer 2 interfaces (switch ports or port channels) where one interface is configured to act as a backup to the other. The feature provides an alternative solution to the Spanning Tree Protocol (STP). Users can disable STP and still retain basic link redundancy. Flex Links are typically configured in service provider or enterprise networks where customers do not want to run STP on the switch. If the switch is running STP, Flex Links is not necessary because STP already provides link-level redundancy or backup.
You configure Flex Links on one Layer 2 interface (the active link) by assigning another Layer 2 interface as the Flex Link or backup link. When one of the links is up and forwarding traffic, the other link is in standby mode, ready to begin forwarding traffic if the other link shuts down. At any given time, only one of the interfaces is in the linkup state and forwarding traffic. If the primary link shuts down, the standby link starts forwarding traffic. When the active link comes back up, it goes into standby mode and does not forward traffic. STP is disabled on Flex Link interfaces.

In Figure 19-1, ports 1 and 2 on switch A are connected to uplink switches B and C. Because they are configured as Flex Links, only one of the interfaces is forwarding traffic; the other is in standby mode. If port 1 is the active link, it begins forwarding traffic between port 1 and switch B; the link between port 2 (the backup link) and switch C is not forwarding traffic. If port 1 goes down, port 2 comes up and starts forwarding traffic to switch C. When port 1 comes back up, it goes into standby mode and does not forward traffic; port 2 continues forwarding traffic.

You can also choose to configure a preemption mechanism, specifying the preferred port for forwarding traffic. For example, in the example in Figure 19-1, you can configure the Flex Links pair with preemption mode. In the scenario shown, when port 1 comes back up and has more bandwidth than port 2, port 1 begins forwarding traffic after 60 seconds. Port 2 becomes the standby port. You do this by entering the interface configuration `switchport backup interface preemption mode bandwidth` and `switchport backup interface preemption delay` commands.

Figure 19-1  Flex Links Configuration Example

If a primary (forwarding) link goes down, a trap notifies the network management stations. If the standby link goes down, a trap notifies the users.

Flex Links are supported only on Layer 2 ports and port channels, not on VLANs or on Layer 3 ports.
VLAN Flex Link Load Balancing and Support

VLAN Flex Link load-balancing allows you to configure a Flex Link pair so that both ports simultaneously forward the traffic for some mutually exclusive VLANs. For example, if Flex Link ports are configured for 1-100 VLANs, the traffic of the first 50 VLANs can be forwarded on one port and the rest on the other port. If one of the ports fail, the other active port forwards all the traffic. When the failed port comes back up, it resumes forwarding traffic in the preferred VLANs. This way, apart from providing the redundancy, this Flex Link pair can be used for load balancing. Also, Flex Link VLAN load-balancing does not impose any restrictions on uplink switches.

Figure 19-2  VLAN Flex Links Load Balancing Configuration Example

Flex Link Multicast Fast Convergence

Flex Link Multicast Fast Convergence reduces the multicast traffic convergence time after a Flex Link failure. This is implemented by a combination of these solutions:

- Learning the Other Flex Link Port as the mrouter Port, page 19-3
- Generating IGMP Reports, page 19-4
- Leaking IGMP Reports, page 19-4
- Configuration Examples, page 19-4

Learning the Other Flex Link Port as the mrouter Port

In a typical multicast network, there is a querier for each VLAN. A switch deployed at the edge of a network has one of its Flex Link ports receiving queries. Flex Link ports are also always forwarding at any given time.

A port that receives queries is added as an mrouter port on the switch. An mrouter port is part of all the multicast groups learned by the switch. After a changeover, queries are received by the other Flex Link port. The other Flex Link port is then learned as the mrouter port. After changeover, multicast traffic then flows through the other Flex Link port. To achieve faster convergence of traffic, both Flex Link ports are learned as mrouter ports whenever either Flex Link port is learned as the mrouter port. Both Flex Link ports are always part of multicast groups.

Though both Flex Link ports are part of the groups in normal operation mode, all traffic on the backup port is blocked. So the normal multicast data flow is not affected by the addition of the backup port as an mrouter port. When the changeover happens, the backup port is unblocked, allowing the traffic to flow. In this case, the upstream multicast data flows as soon as the backup port is unblocked.
Generating IGMP Reports

When the backup link comes up after the changeover, the upstream new distribution switch does not start forwarding multicast data, because the port on the upstream router, which is connected to the blocked Flex Link port, is not part of any multicast group. The reports for the multicast groups were not forwarded by the downstream switch because the backup link is blocked. The data does not flow on this port, until it learns the multicast groups, which occurs only after it receives reports.

The reports are sent by hosts when a general query is received, and a general query is sent within 60 seconds in normal scenarios. When the backup link starts forwarding, to achieve faster convergence of multicast data, the downstream switch immediately sends proxy reports for all the learned groups on this port without waiting for a general query.

Leaking IGMP Reports

To achieve multicast traffic convergence with minimal loss, a redundant data path must be set up before the Flex Link active link goes down. This can be achieved by leaking only IGMP report packets on the Flex Link backup link. These leaked IGMP report messages are processed by upstream distribution routers, so multicast data traffic gets forwarded to the backup interface. Because all incoming traffic on the backup interface is dropped at the ingress of the access switch, no duplicate multicast traffic is received by the host. When the Flex Link active link fails, the access switch starts accepting traffic from the backup link immediately. The only disadvantage of this scheme is that it consumes bandwidth on the link between the distribution switches and on the backup link between the distribution and access switches. This feature is disabled by default and can be configured by using the switchport backup interface interface-id multicast fast-convergence command.

When this feature has been enabled at changeover, the switch does not generate the proxy reports on the backup port, which became the forwarding port.

Configuration Examples

These are configuration examples for learning the other Flex Link port as the mrouter port when Flex Link is configured on Gigabit Ethernet0/11 and Gigabit Ethernet0/12, with output for the show interfaces switchport backup command:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitehernet0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface gigabitehernet0/12
Switch(config-if)# exit
Switch(config)# interface gigabitehernet1/0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (G10/11), 100000 Kbit (G10/12)
Mac Address Move Update Vlan : auto
```
This output shows a querier for VLANs 1 and 401, with their queries reaching the switch through Gigabit Ethernet0/11:

```
Switch# show ip igmp snooping querier
Vlan IP Address IGMP Version Port
----------------------------------
1 1.1.1.1 v2 Gi0/11
401 41.41.41.1 v2 Gi0/11
```

Here is output for the `show ip igmp snooping mrouter` command for VLANs 1 and 401:

```
Switch# show ip igmp snooping mrouter
Vlan ports
------- -----
1 Gi1/0/11(dynamic), Gi1/0/12(dynamic)
401 Gi1/0/11(dynamic), Gi1/0/12(dynamic)
```

Similarly, both Flex Link ports are part of learned groups. In this example, Gigabit Ethernet0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups
Vlan Group Type Version Port List
----------------------------------
1 228.1.5.1 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
1 228.1.5.2 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
```

When a host responds to the general query, the switch forwards this report on all the mrouter ports. In this example, when a host sends a report for the group 228.1.5.1, it is forwarded only on Gigabit Ethernet0/11, because the backup port Gigabit Ethernet0/12 is blocked. When the active link, Gigabit Ethernet0/11, goes down, the backup port, Gigabit Ethernet0/12, begins forwarding.

As soon as this port starts forwarding, the switch sends proxy reports for the groups 228.1.5.1 and 228.1.5.2 on behalf of the host. The upstream router learns the groups and starts forwarding multicast data. This is the default behavior of Flex Link. This behavior changes when the user configures fast convergence using the `switchport backup interface gigabitEthernet 0/12 multicast fast-convergence` command. This example shows turning on this feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 0/11
Switch(config-if)# switchport backup interface gigabitethernet 0/12 multicast fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
-----------------------------------------------
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLAN 1 and 401 with their queries reaching the switch through Gigabit Ethernet0/11:

```
Switch# show ip igmp snooping querier
Vlan IP Address IGMP Version Port
----------------------------------
1 1.1.1.1 v2 Gi0/11
401 41.41.41.1 v2 Gi0/11
```
Understanding Flex Links and the MAC Address-Table Move Update

This is output for the `show ip igmp snooping mrouter` command for VLAN 1 and 401:

```
Switch# show ip igmp snooping mrouter
Vlan  ports
----  -----  
1     Gi0/11(dynamic), Gi0/12(dynamic)
401   Gi10/11(dynamic), Gi0/12(dynamic)
```

Similarly, both the Flex Link ports are a part of the learned groups. In this example, Gigabit Ethernet0/11 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups
Vlan Group Type Version Port List
---------------------------
1   228.1.5.1 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
1   228.1.5.2 igmp v2 Gi1/0/11, Gi1/0/12, Gi2/0/11
```

Whenever a host responds to the general query, the switch forwards this report on all the mrouter ports. When you turn on this feature through the command-line port, and when a report is forwarded by the switch on GigabitEthernet0/11, it is also leaked to the backup port GigabitEthernet0/12. The upstream router learns the groups and starts forwarding multicast data, which is dropped at the ingress because GigabitEthernet0/12 is blocked. When the active link, GigabitEthernet0/11, goes down, the backup port, GigabitEthernet0/12, begins forwarding. You do not need to send any proxy reports because the multicast data is already being forwarded by the upstream router. By leaking reports to the backup port, a redundant multicast path has been set up, and the time taken for the multicast traffic convergence is minimal.

MAC Address-Table Move Update

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence when a primary (forwarding) link goes down and the standby link begins forwarding traffic.

In Figure 19-3, switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and D through a Flex Link pair. Port 1 is forwarding traffic, and port 2 is in the backup state. Traffic from the PC to the server is forwarded from port 1 to port 3. The MAC address of the PC has been learned on port 3 of switch C. Traffic from the server to the PC is forwarded from port 3 to port 1.

If the MAC address-table move update feature is not configured and port 1 goes down, port 2 starts forwarding traffic. However, for a short time, switch C keeps forwarding traffic from the server to the PC through port 3, and the PC does not get the traffic because port 1 is down. If switch C removes the MAC address of the PC on port 3 and relearns it on port 4, traffic can then be forwarded from the server to the PC through port 2.

If the MAC address-table move update feature is configured and enabled on the switches in Figure 19-3 and port 1 goes down, port 2 starts forwarding traffic from the PC to the server. The switch sends a MAC address-table move update packet from port 2. Switch C gets this packet on port 4 and immediately learns the MAC address of the PC on port 4, which reduces the reconvergence time.

You can configure the access switch, switch A, to send MAC address-table move update messages. You can also configure the uplink switches B, C, and D to get and process the MAC address-table move update messages. When switch C gets a MAC address-table move update message from switch A, switch C learns the MAC address of the PC on port 4. Switch C updates the MAC address table, including the forwarding table entry for the PC.

Switch A does not need to wait for the MAC address-table update. The switch detects a failure on port 1 and immediately starts forwarding server traffic from port 2, the new forwarding port. This change occurs in 100 milliseconds (ms). The PC is directly connected to switch A, and the connection status does not change. Switch A does not need to update the PC entry in the MAC address table.
Configuring Flex Links and the MAC Address-Table Move Update

These sections contain this information:

- Default Configuration, page 19-8
- Configuration Guidelines, page 19-8
- Configuring Flex Links, page 19-9
- Configuring VLAN Load Balancing on Flex Links, page 19-11
- Configuring the MAC Address-Table Move Update Feature, page 19-12
Default Configuration

The Flex Links are not configured, and there are no backup interfaces defined.
The preemption mode is off.
The preemption delay is 35 seconds.
The MAC address-table move update feature is not configured on the switch.

Configuration Guidelines

Follow these guidelines to configure Flex Links:

- You can configure up to 16 backup links.
- You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.
- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- A backup link does not have to be the same type (Fast Ethernet, Gigabit Ethernet, or port channel) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- STP is disabled on Flex Link ports. A Flex Link port does not participate in STP, even if the VLANs present on the port are configured for STP. When STP is not enabled, be sure that there are no loops in the configured topology. Once the Flex Link configurations are removed, STP is re-enabled on the ports.

Follow these guidelines to configure VLAN load balancing on the Flex Links feature:

- For Flex Link VLAN load balancing, you must choose the preferred VLANs on the backup interface.
- You cannot configure a preemption mechanism and VLAN load balancing for the same Flex Links pair.

Follow these guidelines to configure the MAC address-table move update feature:

- You can enable and configure this feature on the access switch to send the MAC address-table move updates.
- You can enable and configure this feature on the uplink switches to receive the MAC address-table move updates.
Configuring Flex Links

Beginning in privileged EXEC mode, follow these steps to configure a pair of Flex Links:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport backup interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show interfaces [interface-id] switchport backup</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup config</td>
</tr>
</tbody>
</table>

To disable a Flex Link backup interface, use the no switchport backup interface interface-id interface configuration command.

This example shows how to configure an interface with a backup interface and to verify the configuration:

Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2
Switch(conf-if)# end

Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

<table>
<thead>
<tr>
<th>Active Interface</th>
<th>Backup Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/1</td>
<td>GigabitEthernet0/3</td>
<td>Active Standby/Backup Up</td>
</tr>
<tr>
<td>Vlans Preferred on Active Interface: 1-3,5-4094</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vlans Preferred on Backup Interface: 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to configure a preemption scheme for a pair of Flex Links:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport backup interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport backup interface interface-id preemption mode [forced</td>
</tr>
<tr>
<td></td>
<td>bandwidth</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>switchport backup interface interface-id preemption delay delay-time</td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show interfaces [interface-id] switchport backup</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup config</td>
</tr>
</tbody>
</table>

To remove a preemption scheme, use the no switchport backup interface interface-id preemption mode interface configuration command. To reset the delay time to the default, use the no switchport backup interface interface-id preemption delay interface configuration command.

This example shows how to configure the preemption mode as forced for a backup interface pair and to verify the configuration:

```
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)#switchport backup interface gigabitethernet0/2 preemption mode forced
Switch(conf-if)#switchport backup interface gigabitethernet0/2 preemption delay 50
Switch(conf-if)# end

Switch# show interfaces switchport backup detail
Active Interface Backup Interface State
-------------------------------
GigabitEthernet0/1 GigabitEthernet0/2 Active Up/Backup Standby
Interface Pair : G10/1, G10/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (G10/1), 100000 Kbit (G10/2)
Mac Address Move Update Vlan : auto
```
## Configuring VLAN Load Balancing on Flex Links

Beginning in privileged EXEC mode, follow these steps to configure VLAN load balancing on Flex Links:

<table>
<thead>
<tr>
<th>Command</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> interface interface-id</td>
<td>Specify the interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>The interface can be a physical Layer 2 interface or a port channel.</td>
</tr>
<tr>
<td></td>
<td>(logical interface). The port-channel range is 1 to 48.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport backup interface interface-id prefer vlan vlan-range</td>
<td>Configure a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the interface, and specify the VLANs carried on the interface. The VLAN ID range is 1 to 4094.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show interfaces [interface-id] switchport backup</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup config</td>
<td>(Optional) Save your entries in the switch startup configuration file.</td>
</tr>
</tbody>
</table>

To disable the VLAN load balancing feature, use the `no switchport backup interface interface-id prefer vlan vlan-range` interface configuration command.

In the following example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)#interface gigabitethernet 0/6
Switch(config-if)#switchport backup interface gigabitethernet 0/8 prefer vlan 60,100-120
```

When both interfaces are up, Gi0/8 forwards traffic for VLANs 60 and 100 to 120, and Gi0/6 forwards traffic for VLANs 1 to 50.

```
Switch#show interfaces switchport backup
Switch Backup Interface Pairs:
                      Active Interface        Backup Interface        State
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Up
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
                      Active Interface        Backup Interface        State
GigabitEthernet0/6    GigabitEthernet0/8    Active Down/Backup Up
Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```
When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi0/8 and forwarded on Gi0/6.

Switch#show interfaces switchport backup
Switch Backup Interface Pairs:

<table>
<thead>
<tr>
<th>Active Interface</th>
<th>Backup Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/6</td>
<td>GigabitEthernet0/8</td>
<td>Active Up/Backup Up</td>
</tr>
</tbody>
</table>

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch#show interfaces switchport backup detail
Switch Backup Interface Pairs:

<table>
<thead>
<tr>
<th>Active Interface</th>
<th>Backup Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/3</td>
<td>FastEthernet0/4</td>
<td>Active Down/Backup Up</td>
</tr>
</tbody>
</table>

Vlans Preferred on Active Interface: 1-2, 5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode : off
Bandwidth : 10000 Kbit (Fa0/3), 100000 Kbit (Fa0/4)
Mac Address Move Update Vlan : auto

### Configuring the MAC Address-Table Move Update Feature

This section contains this information:

- Configuring a switch to send MAC address-table move updates
- Configuring a switch to get MAC address-table move updates

Beginning in privileged EXEC mode, follow these steps to configure an access switch to send MAC address-table move updates:

<table>
<thead>
<tr>
<th>Command</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> interface interface-id</td>
<td>Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport backup interface interface-id</td>
<td>Configure a physical Layer 2 interface (or port channel), as part of a Flex Link pair with the interface. The MAC address-table move update VLAN is the lowest VLAN ID on the interface.</td>
</tr>
<tr>
<td>or switchport backup interface interface-id mmu primary vlan vlan-id</td>
<td>Configure a physical Layer 2 interface (or port channel) and specify the VLAN ID on the interface, which is used for sending the MAC address-table move update. When one link is forwarding traffic, the other interface is in standby mode.</td>
</tr>
</tbody>
</table>
To disable the MAC address-table move update feature, use the `no mac address-table move update transmit` interface configuration command. To display the MAC address-table move update information, use the `show mac address-table move update` privileged EXEC command.

This example shows how to configure an access switch to send MAC address-table move update messages:

```
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

This example shows how to verify the configuration:

```
Switch# show mac address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 5
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 000b.462d.c502
Rcv last switch-ID : 0403.fd6a.8700
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

Beginning in privileged EXEC mode, follow these steps to configure a switch to get and process MAC address-table move update messages:

<table>
<thead>
<tr>
<th>Command</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> mac address-table move update receive</td>
<td>Enable the switch to get and process the MAC address-table move updates.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To disable the MAC address-table move update feature, use the `no mac address-table move update receive` configuration command. To display the MAC address-table move update information, use the `show mac address-table move update` privileged EXEC command.

This example shows how to configure a switch to get and process MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

### Monitoring Flex Links and the MAC Address-Table Move Update

Table 19-1 shows the privileged EXEC commands for monitoring the Flex Links configuration and the MAC address-table move update information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces [interface-id] switchport backup</code></td>
<td>Displays the Flex Link backup interface configured for an interface or all the configured Flex Links and the state of each active and backup interface (up or standby mode). When VLAN load balancing is enabled, the output displays the preferred VLANS on Active and Backup interfaces.</td>
</tr>
<tr>
<td><code>show mac address-table move update</code></td>
<td>Displays the MAC address-table move update information on the switch.</td>
</tr>
</tbody>
</table>
Configuring DHCP Features and IP Source Guard Features

This chapter describes how to configure DHCP snooping and option-82 data insertion, and the DHCP server port-based address allocation features on the Catalyst 3560 switch. It also describes how to configure the IP source guard feature.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release, and see the “DHCP Commands” section in the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:
- Understanding DHCP Snooping, page 20-1
- Configuring DHCP Snooping, page 20-9
- Displaying DHCP Snooping Information, page 20-16
- Understanding IP Source Guard, page 20-17
- Configuring IP Source Guard, page 20-19
- Displaying IP Source Guard Information, page 20-26
- Understanding DHCP Server Port-Based Address Allocation, page 20-27
- Configuring DHCP Server Port-Based Address Allocation, page 20-27
- Displaying DHCP Server Port-Based Address Allocation, page 20-30

Understanding DHCP Snooping

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses.

These sections contain this information:
- DHCP Server, page 20-2
- DHCP Relay Agent, page 20-2
Understanding DHCP Snooping

- DHCP Snooping, page 20-2
- Option-82 Data Insertion, page 20-4
- Cisco IOS DHCP Server Database, page 20-7
- DHCP Snooping Binding Database, page 20-8

For information about the DHCP client, see the “Configuring DHCP” section of the “IP Addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides.

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.

DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces.

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Note

For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

An untrusted DHCP message is a message that is received from outside the network or firewall. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer’s switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, a trusted interface is connected to a port on a device in the same network. An untrusted interface is connected to an untrusted interface in the network or to an interface on a device that is not in the network.
Understanding DHCP Snooping

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCPRELEASE or DHCPCLOSELDELETE 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 option-82 information is inserted by an edge switch in software releases earlier than Cisco IOS Release 12.2(25)SEA, you cannot configure DHCP snooping on an aggregation switch because the DHCP snooping bindings database is not properly populated. You also cannot configure IP source guard and dynamic Address Resolution Protocol (ARP) inspection on the switch unless you use static bindings or ARP access control lists (ACLs).

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.
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 and on the VLANs to which subscriber devices using this feature are assigned.

Figure 20-1 is an example of 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, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier, `vlan-mod-port`, from which the packet is received.
- 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 in Figure 20-2 do not change:

• 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 ports and small form-factor pluggable (SFP) module slots, port 3 is the Fast Ethernet 0/1 port, port 4 is the Fast Ethernet 0/2 port, and so forth. Port 27 is the SFP module slot 0/1, and so forth.

Figure 20-2 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 20-2  Suboption Packet Formats

Circuit ID Suboption Frame Format

<table>
<thead>
<tr>
<th>Suboption Type</th>
<th>Circuit ID Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>VLAN</td>
<td>Module</td>
</tr>
</tbody>
</table>

1 byte 1 byte 2 bytes 1 byte 1 byte

Remote ID Suboption Frame Format

<table>
<thead>
<tr>
<th>Suboption Type</th>
<th>Remote ID Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>MAC address</td>
<td>6 bytes</td>
</tr>
</tbody>
</table>

1 byte 1 byte 1 byte 1 byte 6 bytes

Figure 20-3 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 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides.
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 8192 bindings.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP inspection or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch updates the file when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file with bindings:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
<entry-n> <checksum-1-2-..-n>
END
```

Each entry in the file is tagged with a checksum value that the switch uses to verify the entries when it reads the file. The initial-checksum entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E interface-id 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB6488B interface-id 1b6b223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB interface-id 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.

**Configuring DHCP Snooping**

These sections contain this configuration information:

- Default DHCP Snooping Configuration, page 20-10
- DHCP Snooping Configuration Guidelines, page 20-10
- Configuring the DHCP Relay Agent, page 20-11
- Specifying the Packet Forwarding Address, page 20-12
- Enabling DHCP Snooping and Option 82, page 20-13
- Enabling DHCP Snooping on Private VLANs, page 20-15
- Enabling the Cisco IOS DHCP Server Database, page 20-15
- Enabling the DHCP Snooping Binding Database Agent, page 20-15
Default DHCP Snooping Configuration

Table 20-1 shows the default DHCP snooping configuration.

Table 20-1  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 configuration¹</td>
</tr>
<tr>
<td>DHCP relay agent</td>
<td>Enabled²</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)²</td>
</tr>
<tr>
<td>DHCP relay agent forwarding policy</td>
<td>Replace the existing relay agent information²</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 interfaces³</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. 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. This feature is operational only when a destination is configured.</td>
</tr>
</tbody>
</table>

¹  The switch responds to DHCP requests only if it is configured as a DHCP server.
²  The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
³  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

These are the configuration guidelines for DHCP snooping.

- You must globally enable DHCP snooping on the switch.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- 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.
- Before configuring the DHCP snooping information option on your switch, be sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.
- When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or the flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.
• Before configuring the DHCP relay agent on your switch, make sure to configure the device that is acting as the DHCP server. For example, 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 the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.

• 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.

• Follow these guidelines when configuring the DHCP snooping binding database:
  – 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 NTP. For more information, see the “Configuring NTP” section on page 6-4.
  – If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

• Do not enter the ip dhcp snooping information option allow-untrusted command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

• 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.

Note
Do not enable Dynamic Host Configuration Protocol (DHCP) snooping on RSPAN VLANs. If DHCP snooping is enabled on RSPAN VLANs, DHCP packets might not reach the RSPAN destination port.

Configuring the DHCP Relay Agent

Beginning in privileged EXEC mode, follow these steps to enable the DHCP relay agent on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>service dhcp</td>
<td>Enable the DHCP server and relay agent on your switch. By default, this feature is enabled.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To disable the DHCP server and relay agent, use the `no service dhcp` global configuration command.

See the “Configuring DHCP” section of the “IP Addressing and Services” section of the Cisco IOS IP Configuration Guide, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides for these procedures:

- Checking (validating) the relay agent information
- Configuring the relay agent forwarding policy

### 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface vlan vlan-id</strong></td>
</tr>
<tr>
<td></td>
<td>Create a switch virtual interface by entering a VLAN ID, and enter</td>
</tr>
<tr>
<td></td>
<td>interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ip address ip-address subnet-mask</strong></td>
</tr>
<tr>
<td></td>
<td>Configure the interface with an IP address and an IP subnet.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>ip helper-address address</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the DHCP packet forwarding address.</td>
</tr>
<tr>
<td></td>
<td>The helper address can be a specific DHCP server address, or it can be</td>
</tr>
<tr>
<td></td>
<td>the network address if other DHCP servers are on the destination network</td>
</tr>
<tr>
<td></td>
<td>segment. Using the network address enables other servers to respond to</td>
</tr>
<tr>
<td></td>
<td>DHCP requests. If you have multiple servers, you can configure one</td>
</tr>
<tr>
<td></td>
<td>helper address for each server.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>interface range port-range</strong></td>
</tr>
<tr>
<td></td>
<td>Configure multiple physical ports that are connected to the DHCP</td>
</tr>
<tr>
<td></td>
<td>clients, and enter interface range configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>or</strong></td>
</tr>
<tr>
<td></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td>Configure a single physical port that is connected to the DHCP client,</td>
</tr>
<tr>
<td></td>
<td>and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>switchport mode access</strong></td>
</tr>
<tr>
<td></td>
<td>Define the VLAN membership mode for the port.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>switchport access vlan vlan-id</strong></td>
</tr>
<tr>
<td></td>
<td>Assign the ports to the same VLAN as configured in Step 2.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring DHCP Snooping

To remove the DHCP packet forwarding address, use the `no ip helper-address address` interface configuration command.

Enabling DHCP Snooping and Option 82

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip dhcp snooping</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip dhcp snooping vlan vlan-range</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip dhcp snooping information option</td>
</tr>
<tr>
<td>Step 5</td>
<td>ip dhcp snooping information option format remote-id [string ASCII-string</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>hostname]</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip dhcp snooping information option allow-untrusted</td>
</tr>
<tr>
<td>Step 7</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>
To disable DHCP snooping, use the `no ip dhcp snooping` global configuration command. To disable DHCP snooping on a VLAN or range of VLANs, use the `no ip dhcp snooping vlan vlan-range` global configuration command. To disable the insertion and the removal of the option-82 field, use the `no ip dhcp snooping information option` global configuration command. To configure an aggregation switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, use the `no ip dhcp snooping information option allow-untrusted` global configuration command.

This example shows how to enable DHCP snooping globally and on VLAN 10 and to configure a rate limit of 100 packets per second on a port:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping information option
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip dhcp snooping limit rate 100
```
**Enabling DHCP Snooping on Private VLANs**

You can enable DHCP snooping on private VLANs. If DHCP snooping is enabled, the configuration is propagated to both a primary VLAN and its associated secondary VLANs. If DHCP snooping is enabled on the primary VLAN, it is also configured on the secondary VLANs.

If DHCP snooping is already configured on the primary VLAN and you configure DHCP snooping with different settings on a secondary VLAN, the configuration for the secondary VLAN does not take effect. You must configure DHCP snooping on the primary VLAN. If DHCP snooping is not configured on the primary VLAN, this message appears when you are configuring DHCP snooping on the secondary VLAN, such as VLAN 200:

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take effect on secondary vlan 200. DHCP Snooping configuration on secondary vlan is derived from its primary vlan.
```

The `show ip dhcp snooping` privileged EXEC command output shows all VLANs, including primary and secondary private VLANs, on which DHCP snooping is enabled.

**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 12.2* from the Cisco.com page under **Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides.**

**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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip dhcp snooping database</td>
</tr>
<tr>
<td></td>
<td>[flash://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>host-ip][/directory]/image-name.tar</td>
</tr>
<tr>
<td></td>
<td>rcp://user@host/filename</td>
</tr>
<tr>
<td></td>
<td>tftp://host/filename</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip dhcp snooping database timeout seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip dhcp snooping database</td>
</tr>
<tr>
<td></td>
<td>[flash://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>host-ip][/directory]/image-name.tar</td>
</tr>
<tr>
<td></td>
<td>rcp://user@host/filename</td>
</tr>
<tr>
<td></td>
<td>tftp://host/filename</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip dhcp snooping database timeout seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Displaying DHCP Snooping Information

To display the DHCP snooping information, use the privileged EXEC commands in Table 20-2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</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.
Understanding IP Source Guard

IPSG is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor.

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. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

Note

The port ACL takes precedence over any router ACLs or VLAN maps that affect the same interface.

The IP source binding table bindings are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address with its associated MAC address and VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IPSG is supported only on Layer 2 ports, including access and trunk ports. You can configure IPSG with source IP address filtering or with source IP and MAC address filtering.

- Source IP Address Filtering, page 20-17
- Source IP and MAC Address Filtering, page 20-17
- IP Source Guard for Static Hosts, page 20-18

Source IP Address Filtering

When IPSG is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

When a DHCP snooping binding or static IP source binding is added, changed, or deleted on an interface, the switch modifies the port ACL by using the IP source binding changes and re-applies the port ACL to the interface.

If you enable IPSG on an interface on which IP source bindings (dynamically learned by DHCP snooping or manually configured) are not configured, the switch creates and applies a port ACL that denies all IP traffic on the interface. If you disable IP source guard, the switch removes the port ACL from the interface.

Source IP and MAC Address Filtering

IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table.

When address filtering is enabled, the switch filters IP and non-IP traffic. If the source MAC address of an IP or non-IP packet matches a valid IP source binding, the switch forwards the packet. The switch drops all other types of packets except DHCP packets.

The switch uses port security to filter source MAC addresses. The interface can shut down when a port-security violation occurs.
### IP Source Guard for Static Hosts

**Note**
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 `show ip device tracking all` EXEC command, the IP device tracking table displays the entries as ACTIVE.

**Note**
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.
Configuring IP Source Guard

- Default IP Source Guard Configuration, page 20-19
- IP Source Guard Configuration Guidelines, page 20-19
- Enabling IP Source Guard, page 20-20
- Configuring IP Source Guard for Static Hosts, page 20-21

Default IP Source Guard Configuration

By default, IP source guard is disabled.

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.

- If you enable IP source guard with source IP and MAC address filtering, DHCP snooping and port security must be enabled on the interface. You must also enter the `ip dhcp snooping information option` global configuration command and ensure that the DHCP server supports option 82. When IP source guard is enabled with MAC address filtering, the DHCP host MAC address is not learned until the host is granted a lease. When forwarding packets from the server to the host, DHCP snooping uses option-82 data to identify the host port.
- When configuring IP source guard on interfaces on which a private VLAN is configured, port security is not supported.
- IP source guard is not supported on EtherChannels.
- You can enable this feature when 802.1x port-based authentication is enabled.
- If the number of ternary content addressable memory (TCAM) entries exceeds the maximum, the CPU usage increases.
## Enabling IP Source Guard

Begin in privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command</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> interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip verify source</td>
<td>Enable IP source guard with source IP address filtering.</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip source binding mac-address vlan vlan-id ip-address interface interface-id</td>
<td>Add a static IP source binding. Enter this command for each static binding.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show ip verify source [interface interface-id]</td>
<td>Verify the IP source guard configuration.</td>
</tr>
<tr>
<td><strong>Step 8</strong> show ip source binding [ip-address] [mac-address] [dhcp-snooping</td>
<td>static] [interface interface-id] [vlan vlan-id]</td>
</tr>
<tr>
<td><strong>Step 9</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Command Purpose

**Step 1**

**configure terminal**

Enter global configuration mode.

**Step 2**

**interface interface-id**

Specify the interface to be configured, and enter interface configuration mode.

**Step 3**

**ip verify source**

Enable IP source guard with source IP address filtering.

**Step 4**

**exit**

Return to global configuration mode.

**Step 5**

**ip source binding mac-address vlan vlan-id ip-address interface interface-id**

Add a static IP source binding. Enter this command for each static binding.

**Step 6**

**end**

Return to privileged EXEC mode.

**Step 7**

**show ip verify source [interface interface-id]**

Verify the IP source guard configuration.

**Step 8**

**show ip source binding [ip-address] [mac-address] [dhcp-snooping | static] [interface interface-id] [vlan vlan-id]**

Display the IP source bindings on the switch, on a specific VLAN, or on a specific interface.

**Step 9**

**copy running-config startup-config**

(Optional) Save your entries in the configuration file.

To disable IP source guard with source IP address filtering, use the **no ip verify source** interface configuration command.

To delete a static IP source binding entry, use the **no ip source** global configuration command.

This example shows how to enable IP source guard with source IP and MAC filtering on VLANs 10 and 11:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface gigabitethernet0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet0/1
Switch(config)# end
```
Configuring IP Source Guard for Static Hosts

- Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port, page 20-21
- Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port, page 20-24

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. This requirement also applies to IPSG with static hosts on a private VLAN host port.

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</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> ip device tracking</td>
<td>Turn on the IP host table, and globally enable IP device tracking.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport mode access</td>
<td>Configure a port as access.</td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport access vlan vlan-id</td>
<td>Configure the VLAN for this port.</td>
</tr>
<tr>
<td><strong>Step 6</strong> ip verify source tracking port-security</td>
<td>Enable IPSG for static hosts with MAC address filtering. Note When you enable both IP source guard and port security by using the <strong>ip verify source port-security</strong> interface configuration command:</td>
</tr>
<tr>
<td><strong>Step 7</strong> ip device tracking maximum number</td>
<td>Establish 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 <strong>ip device tracking maximum limit-number</strong> interface configuration command.</td>
</tr>
<tr>
<td><strong>Step 8</strong> switchport port-security</td>
<td>(Optional) Activate port security for this port.</td>
</tr>
<tr>
<td><strong>Step 9</strong> switchport port-security maximum value</td>
<td>(Optional) Establish a maximum of MAC addresses for this port.</td>
</tr>
<tr>
<td><strong>Step 10</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 20  Configuring DHCP Features and IP Source Guard Features

Configuring IP Source Guard

This example shows how to enable IPSG with static hosts on a port.

Switch(config)# ip device tracking
Switch(config)# ip device tracking max 10
Switch(config-if)# ip verify source tracking port-security

This example shows how to enable IPSG for static hosts with IP-MAC filters on a Layer 2 access port, to verify the valid IP-MAC bindings on the interface Gi0/3:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

This example shows how to enable IPSG for static hosts with IP-MAC filters on a Layer 2 access port, to verify the valid IP-MAC bindings on the interface Gi0/3, and to verify that the number of bindings on this interface has reached the maximum:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end

Step 11
show ip verify source interface interface-id
Purpose
Verify the configuration and display IPSG permit ACLs for static hosts.

Step 12
show ip device track all [active | inactive] count
Purpose
Verify the configuration by displaying the IP-to-MAC binding for a given host on the switch interface.

- all active—display only the active IP or MAC binding entries
- all inactive—display only the inactive IP or MAC binding entries
- all—display the active and inactive IP or MAC binding entries

This example shows how to stop IPSG with static hosts on an interface.

Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
### Configuring IP Source Guard

This example displays all IP or MAC binding entries for all interfaces. The CLI displays all active as well as inactive entries. When a host is learned on a interface, the new entry is marked as active. When the same host is disconnected from that interface and connected to a different interface, a new IP or MAC binding entry displays as active as soon as the host is detected. The old entry for this host on the previous interface is marked as INACTIVE.

**Switch# show ip verify source**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter-type</th>
<th>Filter-mode</th>
<th>IP-address</th>
<th>Mac-address</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/3</td>
<td>ip-mac trk</td>
<td>active</td>
<td>40.1.1.24</td>
<td>00:00:00:00:03:04</td>
<td>1</td>
</tr>
<tr>
<td>Gi0/3</td>
<td>ip-mac trk</td>
<td>active</td>
<td>40.1.1.20</td>
<td>00:00:00:00:03:05</td>
<td>1</td>
</tr>
<tr>
<td>Gi0/3</td>
<td>ip-mac trk</td>
<td>active</td>
<td>40.1.1.21</td>
<td>00:00:00:00:03:06</td>
<td>1</td>
</tr>
<tr>
<td>Gi0/3</td>
<td>ip-mac trk</td>
<td>active</td>
<td>40.1.1.22</td>
<td>00:00:00:00:03:07</td>
<td>1</td>
</tr>
<tr>
<td>Gi0/3</td>
<td>ip-mac trk</td>
<td>active</td>
<td>40.1.1.23</td>
<td>00:00:00:00:03:08</td>
<td>1</td>
</tr>
</tbody>
</table>

This example displays all active IP or MAC binding entries for all interfaces:

**Switch# show ip device tracking all active**

---

This example displays all active IP or MAC binding entries for all interfaces:

**Switch# show ip device tracking all active**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Vlan</th>
<th>Interface</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.1.1.1</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.2</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.3</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.4</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.5</td>
<td>0001.0600.0000</td>
<td>9</td>
<td>GigabitEthernet0/1</td>
<td>ACTIVE</td>
</tr>
<tr>
<td>200.1.1.6</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.7</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
</tbody>
</table>
This example displays all inactive IP or MAC binding entries for all interfaces. The host was first learned on GigabitEthernet 0/1 and then moved to GigabitEthernet 0/2. The IP or MAC binding entries learned on GigabitEthernet 0/1 are marked as inactive.

Switch# show ip device tracking all inactive
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Vlan</th>
<th>Interface</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.1.1.8</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.9</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.10</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.1</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.3</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.4</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.5</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.6</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>200.1.1.7</td>
<td>0001.0600.0000</td>
<td>8</td>
<td>GigabitEthernet0/1</td>
<td>INACTIVE</td>
</tr>
</tbody>
</table>

This example displays the count of all IP device tracking host entries for all interfaces:

Switch# show ip device tracking all count
Total IP Device Tracking Host entries: 5

<table>
<thead>
<tr>
<th>Interface</th>
<th>Maximum Limit</th>
<th>Number of Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gl0/3</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring IP Source Guard for Static Hosts on a Private VLAN Host Port

**Note**

You must globally 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 setting an IP device tracking maximum on that interface, IPSG with static hosts will reject all the IP traffic from that interface. This requirement also applies to IPSG with static hosts on a Layer 2 access port.

Beginning in privileged EXEC mode, follow these steps to configure IPSG for static hosts with IP filters on a Layer 2 access port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>vlan vlan-id1</td>
<td>Enter VLAN configuration mode.</td>
</tr>
<tr>
<td>private-vlan primary</td>
<td>Establish a primary VLAN on a private VLAN port.</td>
</tr>
<tr>
<td>exit</td>
<td>Exit VLAN configuration mode.</td>
</tr>
<tr>
<td>vlan vlan-id2</td>
<td>Enter configuration VLAN mode for another VLAN.</td>
</tr>
<tr>
<td>private-vlan isolated</td>
<td>Establish an isolated VLAN on a private VLAN port.</td>
</tr>
<tr>
<td>exit</td>
<td>Exit VLAN configuration mode.</td>
</tr>
<tr>
<td>vlan vlan-id1</td>
<td>Enter configuration VLAN mode.</td>
</tr>
<tr>
<td>private-vlan association 201</td>
<td>Associate the VLAN on an isolated private VLAN port.</td>
</tr>
</tbody>
</table>
Chapter 20  Configuring DHCP Features and IP Source Guard Features

Configuring IP Source Guard

Step 10 exit
Exit VLAN configuration mode.

Step 11 interface fastEthernet interface-id
Enter interface configuration mode.

Step 12 switchport mode private-vlan host
(Optional) Establish a port as a private VLAN host.

Step 13 switchport private-vlan host-association vlan-id1 vlan-id2
(Optional) Associate this port with the corresponding private VLAN.

Step 14 ip device tracking maximum number
Establish a maximum for the number of static IPs that the IP device tracking table allows on the port.
The maximum is 10.

Note You must globally configure the ip device tracking maximum number interface command for IPSG for static hosts to work.

Step 15 ip verify source tracking [port-security]
Activate IPSG for static hosts with MAC address filtering on this port.

Step 16 end
Exit configuration interface mode.

Step 17 show ip device tracking all
Verify the configuration.

Step 18 show ip verify source interface interface-id
Verify the IP source guard configuration. Display IPSG permit ACLs for static hosts.

This example shows how to enable IPSG for static hosts with IP filters on a private VLAN host port:

Switch(config)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 201
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# private-vlan association 201
Switch(config-vlan)# exit
Switch(config)# int fastEthernet 4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 200 201
Switch(config-if)# ip device tracking maximum 8
Switch(config-if)# ip verify source tracking

Switch# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
---------------------------------------------------------------------
IP Address       MAC Address       Vlan Interface    STATE
---------------------------------------------------------------------
40.1.1.24        0000.0000.0304    200 FastEthernet0/3  ACTIVE
40.1.1.20        0000.0000.0305    200 FastEthernet0/3  ACTIVE
40.1.1.21        0000.0000.0306    200 FastEthernet0/3  ACTIVE
40.1.1.22        0000.0000.0307    200 FastEthernet0/3  ACTIVE
40.1.1.23        0000.0000.0308    200 FastEthernet0/3  ACTIVE
The output shows the five valid IP-MAC bindings that have been learned on the interface Fa0/3. For the private VLAN cases, the bindings are associated with primary VLAN ID. So, in this example, the primary VLAN ID, 200, is shown in the table.

Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Fa0/3      ip trk       active       40.1.1.23                           200
Fa0/3      ip trk       active       40.1.1.24                           200
Fa0/3      ip trk       active       40.1.1.20                           200
Fa0/3      ip trk       active       40.1.1.21                           200
Fa0/3      ip trk       active       40.1.1.22                           200
Fa0/3      ip trk       active       40.1.1.23                           201
Fa0/3      ip trk       active       40.1.1.24                           201
Fa0/3      ip trk       active       40.1.1.20                           201
Fa0/3      ip trk       active       40.1.1.21                           201
Fa0/30/3    ip trk       active       40.1.1.22                           201

The output shows that the five valid IP-MAC bindings are on both the primary and secondary VLAN.

Displaying IP Source Guard Information

To display the IP source guard information, use one or more of the privileged EXEC commands in Table 20-3:

Table 20-3  Commands for Displaying IP Source Guard Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip device tracking</td>
<td>Display the active IP or MAC binding entries for all interfaces.</td>
</tr>
<tr>
<td>show ip source binding</td>
<td>Display the IP source bindings on a switch.</td>
</tr>
<tr>
<td>show ip verify source</td>
<td>Display the IP source guard configuration on the switch.</td>
</tr>
</tbody>
</table>
Understanding 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.

Configuring DHCP Server Port-Based Address Allocation

This section contains this configuration information:

- Default Port-Based Address Allocation Configuration, page 20-27
- Port-Based Address Allocation Configuration Guidelines, page 20-27
- Enabling DHCP Server Port-Based Address Allocation, page 20-28

Default Port-Based Address Allocation Configuration

By default, DHCP server port-based address allocation is disabled.

Port-Based Address Allocation Configuration Guidelines

These are the configuration guidelines for DHCP port-based address allocation:

- Only one IP address can be assigned per port.
- Reserved addresses (preassigned) cannot be cleared by using the `clear ip dhcp binding` global configuration command.
• Preassigned addresses are automatically excluded from normal dynamic IP address assignment. Preassigned addresses cannot be used in host pools, but there can be multiple preassigned addresses per DHCP address pool.

• 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 DHCP Server Port-Based Address Allocation

Beginning in privileged EXEC mode, follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

<table>
<thead>
<tr>
<th>Command</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> ip dhcp use subscriber-id client-id</td>
<td>Configure the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip dhcp subscriber-id interface-name</td>
<td>Automatically generate a subscriber identifier based on the short name of the interface. A subscriber identifier configured on a specific interface takes precedence over this command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip dhcp server use subscriber-id client-id</td>
<td>Configure the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show running config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 8</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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. To restrict assignments from the DHCP pool to preconfigured reservations, you can enter the reserved-only DHCP pool configuration command. Unreserved addresses that are part of the network or on pool ranges are not offered to the client, and other clients are not served by the pool. By entering this command, users can configure a group of switches with DHCP pools that share a common IP subnet and that ignore requests from clients of other switches.
Beginning in privileged EXEC mode follow these steps to preassign an IP address and to associate it to a client identified by the interface name.

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</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>2</td>
<td><code>ip dhcp pool poolname</code></td>
<td>Enter DHCP pool configuration mode, and define the name for the DHCP pool. The pool name can be a symbolic string (such as Engineering) or an integer (such as 0).</td>
</tr>
<tr>
<td>3</td>
<td>`network network-number [mask</td>
<td>prefix-length]`</td>
</tr>
<tr>
<td>4</td>
<td><code>address ip-address client-id string [ascii]</code></td>
<td>Reserve an IP address for a DHCP client identified by the interface name. string—can be an ASCII value or a hexadecimal value.</td>
</tr>
<tr>
<td>5</td>
<td><code>reserved-only</code></td>
<td>(Optional) Use only reserved addresses in the DHCP address pool. The default is to not restrict pool addresses.</td>
</tr>
<tr>
<td>6</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td><code>show ip dhcp pool</code></td>
<td>Verify DHCP pool configuration.</td>
</tr>
<tr>
<td>8</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable DHCP port-based address allocation, use the `no ip dhcp use subscriber-id client-id` global configuration command. To disable the automatic generation of a subscriber identifier, use the `no ip dhcp subscriber-id interface-name` global configuration command. To disable the subscriber identifier on an interface, use the `no ip dhcp server use subscriber-id client-id` interface configuration command.

To remove an IP address reservation from a DHCP pool, use the `no address ip-address client-id string` DHCP pool configuration command. To change the address pool to nonrestricted, enter the `no reserved-only` DHCP pool configuration command.

In this example, a subscriber identifier is automatically generated, and the DHCP server ignores any client identifier fields in the DHCP messages and uses the subscriber identifier instead. The subscriber identifier is based on the short name of the interface and the client preassigned IP address 10.1.1.7.

```
switch# show running config
Building configuration...
Current configuration : 4899 bytes
!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
```
network 10.1.1.0 255.255.255.0
display 10.1.1.7 client-id "Et1/0" ascii
<output truncated>

This example shows that the preassigned address was correctly reserved in the DHCP pool:

switch# show ip dhcp pool dhcppool
Pool dhcp pool:
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 0
  Excluded addresses : 4
  Pending event : none
  1 subnet is currently in the pool:
  Current index   IP address range         Leased/Excluded/Total
  10.1.1.1        10.1.1.1 - 10.1.1.254     0     / 0 / 254
  1 reserved address is currently in the pool
Address         Client
  10.1.1.7 Et1/0

For more information about configuring the DHCP server port-based address allocation feature, go to Cisco.com, and enter Cisco IOS IP Addressing Services in the Search field to access the Cisco IOS software documentation. You can also access the documentation:

Displaying DHCP Server Port-Based Address Allocation

To display the DHCP server port-based address allocation information, use one or more of the privileged EXEC commands in Table 20-4:

Table 20-4: Commands for Displaying DHCP Port-Based Address Allocation Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface interface id</td>
<td>Display the status and configuration of a specific interface.</td>
</tr>
<tr>
<td>show ip dhcp pool</td>
<td>Display the DHCP address pools.</td>
</tr>
<tr>
<td>show ip dhcp binding</td>
<td>Display address bindings on the Cisco IOS DHCP server.</td>
</tr>
</tbody>
</table>
Configuring Dynamic ARP Inspection

This chapter describes how to configure dynamic Address Resolution Protocol inspection (dynamic ARP inspection) on the Catalyst 3560 switch. This feature helps prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding Dynamic ARP Inspection, page 21-1
- Configuring Dynamic ARP Inspection, page 21-5
- Displaying Dynamic ARP Inspection Information, page 21-15

Understanding Dynamic ARP Inspection

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. For example, Host B wants to send information to Host A but does not have the MAC address of Host A in its ARP cache. Host B generates a broadcast message for all hosts within the broadcast domain to obtain the MAC address associated with the IP address of Host A. All hosts within the broadcast domain receive the ARP request, and Host A responds with its MAC address. However, because ARP allows a gratuitous reply from a host even if an ARP request was not received, an ARP spoofing attack and the poisoning of ARP caches can occur. After the attack, all traffic from the device under attack flows through the attacker’s computer and then to the router, switch, or host.

A malicious user can attack hosts, switches, and routers connected to your Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. Figure 21-1 shows an example of ARP cache poisoning.
Understanding Dynamic ARP Inspection

Hosts A, B, and C are connected to the switch on interfaces A, B, and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, Host A uses IP address IA and MAC address MA. When Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. When the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA; for example, IP address IA is bound to MAC address MA. When Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and the MAC address MB.

Host C can poison the ARP caches of the switch, Host A, and Host B by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic man-in-the-middle attack.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

You enable dynamic ARP inspection on a per-VLAN basis by using the `ip arp inspection vlan vlan-range` global configuration command. For configuration information, see the “Configuring Dynamic ARP Inspection in DHCP Environments” section on page 21-7.

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses. You define an ARP ACL by using the `arp access-list acl-name` global configuration command. For configuration information, see the “Configuring ARP ACLs for Non-DHCP Environments” section on page 21-9. The switch logs dropped packets. For more information about the log buffer, see the “Logging of Dropped Packets” section on page 21-4.
You can configure dynamic ARP inspection to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header. Use the `ip arp inspection validate {src-mac | dst-mac | ip}` global configuration command. For more information, see the “Performing Validation Checks” section on page 21-12.

### Interface Trust States and Network Security

Dynamic ARP inspection associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass all dynamic ARP inspection validation checks, and those arriving on untrusted interfaces undergo the dynamic ARP inspection validation process.

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted. With this configuration, all ARP packets entering the network from a given switch bypass the security check. No other validation is needed at any other place in the VLAN or in the network. You configure the trust setting by using the `ip arp inspection trust` interface configuration command.

**Caution**

Use the trust state configuration carefully. Configuring interfaces as untrusted when they should be trusted can result in a loss of connectivity.

In Figure 21-2, assume that both Switch A and Switch B are running dynamic ARP inspection on the VLAN that includes Host 1 and Host 2. If Host 1 and Host 2 acquire their IP addresses from the DHCP server connected to Switch A, only Switch A binds the IP-to-MAC address of Host 1. Therefore, if the interface between Switch A and Switch B is untrusted, the ARP packets from Host 1 are dropped by Switch B. Connectivity between Host 1 and Host 2 is lost.

**Figure 21-2  ARP Packet Validation on a VLAN Enabled for Dynamic ARP Inspection**

Configuring interfaces to be trusted when they are actually untrusted leaves a security hole in the network. If Switch A is not running dynamic ARP inspection, Host 1 can easily poison the ARP cache of Switch B (and Host 2, if the link between the switches is configured as trusted). This condition can occur even though Switch B is running dynamic ARP inspection.
Dynamic ARP inspection ensures that hosts (on untrusted interfaces) connected to a switch running dynamic ARP inspection do not poison the ARP caches of other hosts in the network. However, dynamic ARP inspection does not prevent hosts in other portions of the network from poisoning the caches of the hosts that are connected to a switch running dynamic ARP inspection.

In cases in which some switches in a VLAN run dynamic ARP inspection and other switches do not, configure the interfaces connecting such switches as untrusted. However, to validate the bindings of packets from nondynamic ARP inspection switches, configure the switch running dynamic ARP inspection with ARP ACLs. When you cannot determine such bindings, at Layer 3, isolate switches running dynamic ARP inspection from switches not running dynamic ARP inspection switches. For configuration information, see the “Configuring ARP ACLs for Non-DHCP Environments” section on page 21-9.

Note

Depending on the setup of the DHCP server and the network, it might not be possible to validate a given ARP packet on all switches in the VLAN.

Rate Limiting of ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack. By default, the rate for untrusted interfaces is 15 packets per second (pps). Trusted interfaces are not rate-limited. You can change this setting by using the `ip arp inspection limit` interface configuration command.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you intervene. You can use the `errdisable recovery` global configuration command to enable error disable recovery so that ports automatically emerge from this state after a specified timeout period.

For configuration information, see the “Limiting the Rate of Incoming ARP Packets” section on page 21-11.

Relative Priority of ARP ACLs and DHCP Snooping Entries

Dynamic ARP inspection uses the DHCP snooping binding database for the list of valid IP-to-MAC address bindings.

ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the `ip arp inspection filter vlan` global configuration command. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Logging of Dropped Packets

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.
You use the `ip arp inspection log-buffer` global configuration command to configure the number of entries in the buffer and the number of entries needed in the specified interval to generate system messages. You specify the type of packets that are logged by using the `ip arp inspection vlan logging` global configuration command. For configuration information, see the “Configuring the Log Buffer” section on page 21-13.

## Configuring Dynamic ARP Inspection

These sections contain this configuration information:

- Default Dynamic ARP Inspection Configuration, page 21-5
- Dynamic ARP Inspection Configuration Guidelines, page 21-6
- Configuring Dynamic ARP Inspection in DHCP Environments, page 21-7 (required in DHCP environments)
- Configuring ARP ACLs for Non-DHCP Environments, page 21-9 (required in non-DHCP environments)
- Limiting the Rate of Incoming ARP Packets, page 21-11 (optional)
- Performing Validation Checks, page 21-12 (optional)
- Configuring the Log Buffer, page 21-13 (optional)

### Default Dynamic ARP Inspection Configuration

Table 21-1 shows the default dynamic ARP inspection configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic ARP inspection</td>
<td>Disabled on all VLANs.</td>
</tr>
<tr>
<td>Interface trust state</td>
<td>All interfaces are untrusted.</td>
</tr>
<tr>
<td>Rate limit of incoming ARP packets</td>
<td>The rate is 15 pps on untrusted interfaces, assuming that the network is a switched network with a host connecting to as many as 15 new hosts per second. The rate is unlimited on all trusted interfaces. The burst interval is 1 second.</td>
</tr>
<tr>
<td>ARP ACLs for non-DHCP environments</td>
<td>No ARP ACLs are defined.</td>
</tr>
<tr>
<td>Validation checks</td>
<td>No checks are performed.</td>
</tr>
<tr>
<td>Log buffer</td>
<td>When dynamic ARP inspection is enabled, all denied or dropped ARP packets are logged. The number of entries in the log is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second.</td>
</tr>
<tr>
<td>Per-VLAN logging</td>
<td>All denied or dropped ARP packets are logged.</td>
</tr>
</tbody>
</table>
Dynamic ARP Inspection Configuration Guidelines

These are the dynamic ARP inspection configuration guidelines:

- Dynamic ARP inspection is an ingress security feature; it does not perform any egress checking.
- Dynamic ARP inspection is not effective for hosts connected to switches that do not support dynamic ARP inspection or that do not have this feature enabled. Because man-in-the-middle attacks are limited to a single Layer 2 broadcast domain, separate the domain with dynamic ARP inspection checks from the one with no checking. This action secures the ARP caches of hosts in the domain enabled for dynamic ARP inspection.
- Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. For configuration information, see Chapter 20, “Configuring DHCP Features and IP Source Guard Features.”

When DHCP snooping is disabled or in non-DHCP environments, use ARP ACLs to permit or to deny packets.

- Dynamic ARP inspection is supported on access ports, trunk ports, EtherChannel ports, and private VLAN ports.

**Note**

Do not enable Dynamic ARP inspection on RSPAN VLANs. If Dynamic ARP inspection is enabled on RSPAN VLANs, Dynamic ARP inspection packets might not reach the RSPAN destination port.

- A physical port can join an EtherChannel port channel only when the trust state of the physical port and the channel port match. Otherwise, the physical port remains suspended in the port channel. A port channel inherits its trust state from the first physical port that joins the channel. Consequently, the trust state of the first physical port need not match the trust state of the channel.

Conversely, when you change the trust state on the port channel, the switch configures a new trust state on all the physical ports that comprise the channel.

- The operating rate for the port channel is cumulative across all the physical ports within the channel. For example, if you configure the port channel with an ARP rate-limit of 400 pps, all the interfaces combined on the channel receive an aggregate 400 pps. The rate of incoming ARP packets on EtherChannel ports is equal to the sum of the incoming rate of packets from all the channel members. Configure the rate limit for EtherChannel ports only after examining the rate of incoming ARP packets on the channel-port members.

The rate of incoming packets on a physical port is checked against the port-channel configuration rather than the physical-ports configuration. The rate-limit configuration on a port channel is independent of the configuration on its physical ports.

If the EtherChannel receives more ARP packets than the configured rate, the channel (including all physical ports) is placed in the error-disabled state.
• Make sure to limit the rate of ARP packets on incoming trunk ports. Configure trunk ports with higher rates to reflect their aggregation and to handle packets across multiple dynamic ARP inspection-enabled VLANs. You also can use the `ip arp inspection limit none` interface configuration command to make the rate unlimited. A high rate-limit on one VLAN can cause a denial-of-service attack to other VLANs when the software places the port in the error-disabled state.

• When you enable dynamic ARP inspection on the switch, policers that were configured to police ARP traffic are no longer effective. The result is that all ARP traffic is sent to the CPU.

### Configuring Dynamic ARP Inspection in DHCP Environments

This procedure shows how to configure dynamic ARP inspection when two switches support this feature. Host 1 is connected to Switch A, and Host 2 is connected to Switch B as shown in Figure 21-2 on page 21-3. Both switches are running dynamic ARP inspection on VLAN 1 where the hosts are located. A DHCP server is connected to Switch A. Both hosts acquire their IP addresses from the same DHCP server. Therefore, Switch A has the bindings for Host 1 and Host 2, and Switch B has the binding for Host 2.

**Note**

Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping to permit ARP packets that have dynamically assigned IP addresses. For configuration information, see Chapter 20, “Configuring DHCP Features and IP Source Guard Features.”

For information on how to configure dynamic ARP inspection when only one switch supports the feature, see the “Configuring ARP ACLs for Non-DHCP Environments” section on page 21-9.
Beginning in privileged EXEC mode, follow these steps to configure dynamic ARP inspection. You must perform this procedure on both switches. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>show cdp neighbors</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip arp inspection vlan vlan-range</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip arp inspection trust</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show ip arp inspection interfaces</td>
</tr>
<tr>
<td></td>
<td>show ip arp inspection vlan vlan-range</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show ip dhcp snooping binding</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>show ip arp inspection statistics vlan vlan-range</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable dynamic ARP inspection, use the **no ip arp inspection vlan vlan-range** global configuration command. To return the interfaces to an untrusted state, use the **no ip arp inspection trust** interface configuration command.

This example shows how to configure dynamic ARP inspection on Switch A in VLAN 1. You would perform a similar procedure on Switch B:

```
Switch(config)# ip arp inspection vlan 1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip arp inspection trust
```
**Configuring ARP ACLs for Non-DHCP Environments**

This procedure shows how to configure dynamic ARP inspection when Switch B shown in Figure 21-2 on page 21-3 does not support dynamic ARP inspection or DHCP snooping.

If you configure port 1 on Switch A as trusted, a security hole is created because both Switch A and Host 1 could be attacked by either Switch B or Host 2. To prevent this possibility, you must configure port 1 on Switch A as untrusted. To permit ARP packets from Host 2, you must set up an ARP ACL and apply it to VLAN 1. If the IP address of Host 2 is not static (it is impossible to apply the ACL configuration on Switch A) you must separate Switch A from Switch B at Layer 3 and use a router to route packets between them.

Beginning in privileged EXEC mode, follow these steps to configure an ARP ACL on Switch A. This procedure is required in non-DHCP environments.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</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>2</td>
<td><code>arp access-list acl-name</code></td>
<td>Define an ARP ACL, and enter ARP access-list configuration mode. By default, no ARP access lists are defined. <strong>Note</strong> At the end of the ARP access list, there is an implicit <code>deny ip any mac any</code> command.</td>
</tr>
</tbody>
</table>
| 3    | `permit ip host sender-ip mac host sender-mac [log]` | Permit ARP packets from the specified host (Host 2).  
• For `sender-ip`, enter the IP address of Host 2.  
• For `sender-mac`, enter the MAC address of Host 2.  
• (Optional) Specify `log` to log a packet in the log buffer when it matches the access control entry (ACE). Matches are logged if you also configure the `matchlog` keyword in the `ip arp inspection vlan logging` global configuration command. For more information, see the “Configuring the Log Buffer” section on page 21-13. |
| 4    | `exit` | Return to global configuration mode. |
### Command Purpose

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|        | ip arp inspection filter *arp-acl-name* vlan *vlan-range* [static] | Apply the ARP ACL to the VLAN. By default, no defined ARP ACLs are applied to any VLAN.  
- For *arp-acl-name*, specify the name of the ACL created in Step 2.  
- For *vlan-range*, specify the VLAN that the switches and hosts are in. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.  
- (Optional) Specify **static** to treat implicit denies in the ARP ACL as explicit denies and to drop packets that do not match any previous clauses in the ACL. DHCP bindings are not used.

If you do not specify this keyword, it means that there is no explicit deny in the ACL that denies the packet, and DHCP bindings determine whether a packet is permitted or denied if the packet does not match any clauses in the ACL. ARP packets containing only IP-to-MAC address bindings are compared against the ACL. Packets are permitted only if the access list permits them. |

<table>
<thead>
<tr>
<th>Step 6</th>
<th>interface <em>interface-id</em></th>
<th>Specify the Switch A interface that is connected to Switch B, and enter interface configuration mode.</th>
</tr>
</thead>
</table>
| Step 7 | no ip arp inspection trust | Configure the Switch A interface that is connected to Switch B as untrusted.  
By default, all interfaces are untrusted.  
For untrusted interfaces, the switch intercepts all ARP requests and responses. It verifies that the intercepted packets have valid IP-to-MAC address bindings before updating the local cache and before forwarding the packet to the appropriate destination. The switch drops invalid packets and logs them in the log buffer according to the logging configuration specified with the **ip arp inspection vlan logging** global configuration command. For more information, see the “Configuring the Log Buffer” section on page 21-13. |

<table>
<thead>
<tr>
<th>Step 8</th>
<th>end</th>
<th>Return to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>show arp access-list [acl-name]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>show ip arp inspection vlan <em>vlan-range</em></td>
<td></td>
</tr>
<tr>
<td></td>
<td>show ip arp inspection interfaces</td>
<td></td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the ARP ACL, use the **no arp access-list** global configuration command. To remove the ARP ACL attached to a VLAN, use the **no ip arp inspection filter *arp-acl-name* vlan *vlan-range*** global configuration command.
This example shows how to configure an ARP ACL called host2 on Switch A, to permit ARP packets from Host 2 (IP address 1.1.1.1 and MAC address 0001.0001.0001), to apply the ACL to VLAN 1, and to configure port 1 on Switch A as untrusted:

Switch(config)# arp access-list host2
Switch(config-arp-acl)# permit ip host 1.1.1.1 mac host 1.1.1
Switch(config-arp-acl)# exit
Switch(config)# ip arp inspection filter host2 vlan 1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no ip arp inspection trust

Limiting the Rate of Incoming ARP Packets

The switch CPU performs dynamic ARP inspection validation checks; therefore, the number of incoming ARP packets is rate-limited to prevent a denial-of-service attack.

When the rate of incoming ARP packets exceeds the configured limit, the switch places the port in the error-disabled state. The port remains in that state until you enable error-disabled recovery so that ports automatically emerge from this state after a specified timeout period.

Note

Unless you configure a rate limit on an interface, changing the trust state of the interface also changes its rate limit to the default value for that trust state. After you configure the rate limit, the interface retains the rate limit even when its trust state is changed. If you enter the no ip arp inspection limit interface configuration command, the interface reverts to its default rate limit.

For configuration guidelines for rate limiting trunk ports and EtherChannel ports, see the “Dynamic ARP Inspection Configuration Guidelines” section on page 21-6.

Beginning in privileged EXEC mode, follow these steps to limit the rate of incoming ARP packets. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip arp inspection limit {rate pps [burst interval seconds]</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>exit</td>
</tr>
</tbody>
</table>
To return to the default rate-limit configuration, use the `no ip arp inspection limit` interface configuration command. To disable error recovery for dynamic ARP inspection, use the `no errdisable recovery cause arp-inspection` global configuration command.

### Performing Validation Checks

Dynamic ARP inspection intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. You can configure the switch to perform additional checks on the destination MAC address, the sender and target IP addresses, and the source MAC address.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** | **errdisable recovery cause**
| | **arp-inspection interval** *interval* |
| | (Optional) Enable error recovery from the dynamic ARP inspection error-disable state.
| | By default, recovery is disabled, and the recovery interval is 300 seconds.
| | For *interval* *interval*, specify the time in seconds to recover from the error-disable state. The range is 30 to 86400.
| **Step 6** | `exit` |
| | Return to privileged EXEC mode.
| **Step 7** | `show ip arp inspection interfaces`
| | `show errdisable recovery`
| | Verify your settings.
| **Step 8** | `copy running-config startup-config`
| | (Optional) Save your entries in the configuration file.
Beginning in privileged EXEC mode, follow these steps to perform specific checks on incoming ARP packets. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | ip arp inspection validate \{[src-mac] [dst-mac] [ip]\} | Perform a specific check on incoming ARP packets. By default, no checks are performed. The keywords have these meanings:  
  - For **src-mac**, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.  
  - For **dst-mac**, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.  
  - For **ip**, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses. You must specify at least one of the keywords. Each command overrides the configuration of the previous command; that is, if a command enables src and dst mac validations, and a second command enables IP validation only, the src and dst mac validations are disabled as a result of the second command. |
| **Step 3** | exit | Return to privileged EXEC mode. |
| **Step 4** | show ip arp inspection vlan vlan-range | Verify your settings. |
| **Step 5** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable checking, use the **no ip arp inspection validate** **[src-mac]** **[dst-mac]** **[ip]** global configuration command. To display statistics for forwarded, dropped, and MAC and IP validation failure packets, use the **show ip arp inspection statistics** privileged EXEC command.

### Configuring the Log Buffer

When the switch drops a packet, it places an entry in the log buffer and then generates system messages on a rate-controlled basis. After the message is generated, the switch clears the entry from the log buffer. Each log entry contains flow information, such as the receiving VLAN, the port number, the source and destination IP addresses, and the source and destination MAC addresses.

A log-buffer entry can represent more than one packet. For example, if an interface receives many packets on the same VLAN with the same ARP parameters, the switch combines the packets as one entry in the log buffer and generates a single system message for the entry.
If the log buffer overflows, it means that a log event does not fit into the log buffer, and the display for the `show ip arp inspection log` privileged EXEC command is affected. A -- in the display appears in place of all data except the packet count and the time. No other statistics are provided for the entry. If you see this entry in the display, increase the number of entries in the log buffer or increase the logging rate.

Beginning in privileged EXEC mode, follow these steps to configure the log buffer. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| `ip arp inspection log-buffer {entries number | logs number interval seconds}` | Configure the dynamic ARP inspection logging buffer. By default, when dynamic ARP inspection is enabled, denied or dropped ARP packets are logged. The number of log entries is 32. The number of system messages is limited to 5 per second. The logging-rate interval is 1 second. The keywords have these meanings:
- For `entries number`, specify the number of entries to be logged in the buffer. The range is 0 to 1024.
- For `logs number interval seconds`, specify the number of entries to generate system messages in the specified interval.
  - For `logs number`, the range is 0 to 1024. A 0 value means that the entry is placed in the log buffer, but a system message is not generated.
  - For `interval seconds`, the range is 0 to 86400 seconds (1 day). A 0 value means that a system message is immediately generated (and the log buffer is always empty).
  - An interval setting of 0 overrides a log setting of 0.

The `logs` and `interval` settings interact. If the `logs number X` is greater than `interval seconds Y`, `X` divided by `Y` (X/Y) system messages are sent every second. Otherwise, one system message is sent every `Y` divided by `X` (Y/X) seconds.
Displaying Dynamic ARP Inspection Information

To display dynamic ARP inspection information, use the privileged EXEC commands described in Table 21-2:

**Table 21-2  Commands for Displaying Dynamic ARP Inspection Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp access-list [acl-name]</td>
<td>Displays detailed information about ARP ACLs.</td>
</tr>
<tr>
<td>show ip arp inspection interfaces [interface-id]</td>
<td>Displays the trust state and the rate limit of ARP packets for the specified interface or all interfaces.</td>
</tr>
<tr>
<td>show ip arp inspection vlan vlan-range</td>
<td>Displays the configuration and the operating state of dynamic ARP inspection for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).</td>
</tr>
</tbody>
</table>
To clear or display dynamic ARP inspection statistics, use the privileged EXEC commands in Table 21-3:

**Table 21-3  Commands for Clearing or Displaying Dynamic ARP Inspection Statistics**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clear ip arp inspection statistics</strong></td>
<td>Clears dynamic ARP inspection statistics.</td>
</tr>
<tr>
<td><strong>show ip arp inspection statistics [vlan vlan-range]</strong></td>
<td>Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified VLAN. If no VLANs are specified or if a range is specified, displays information only for VLANs with dynamic ARP inspection enabled (active).</td>
</tr>
</tbody>
</table>

For the **show ip arp inspection statistics** command, the switch increments the number of forwarded packets for each ARP request and response packet on a trusted dynamic ARP inspection port. The switch increments the number of ACL or DHCP permitted packets for each packet that is denied by source MAC, destination MAC, or IP validation checks, and the switch increments the appropriate failure count.

To clear or display dynamic ARP inspection logging information, use the privileged EXEC commands in Table 21-4:

**Table 21-4  Commands for Clearing or Displaying Dynamic ARP Inspection Logging Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clear ip arp inspection log</strong></td>
<td>Clears the dynamic ARP inspection log buffer.</td>
</tr>
<tr>
<td><strong>show ip arp inspection log</strong></td>
<td>Displays the configuration and contents of the dynamic ARP inspection log buffer.</td>
</tr>
</tbody>
</table>

For more information about these commands, see the command reference for this release.
Configuring IGMP Snooping and MVR

This chapter describes how to configure Internet Group Management Protocol (IGMP) snooping on the Catalyst 3560 switch, including an application of local IGMP snooping, Multicast VLAN Registration (MVR). It also includes procedures for controlling multicast group membership by using IGMP filtering and procedures for configuring the IGMP throttling action.

Note

For IP Version 6 (IPv6) traffic, Multicast Listener Discovery (MLD) snooping performs the same function as IGMP snooping for IPv4 traffic. For information about MLD snooping, see Chapter 39, “Configuring IPv6 MLD Snooping.”

Note

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the “IP Multicast Routing Commands” section in the Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Understanding IGMP Snooping, page 22-2
- Configuring IGMP Snooping, page 22-7
- Displaying IGMP Snooping Information, page 22-16
- Understanding Multicast VLAN Registration, page 22-18
- Configuring MVR, page 22-20
- Displaying MVR Information, page 22-24
- Configuring IGMP Filtering and Throttling, page 22-25
- Displaying IGMP Filtering and Throttling Configuration, page 22-30

Note

You can either manage IP multicast group addresses through features such as IGMP snooping and MVR, or you can use static IP addresses.
Understanding IGMP Snooping

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

Note

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

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The 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, rather than 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. For more information about the IGMP snooping querier, see the “Configuring the IGMP Snooping Querier” section on page 22-14.

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, page 22-3
- Joining a Multicast Group, page 22-3
- Leaving a Multicast Group, page 22-5
- Immediate Leave, page 22-6
- IGMP Configurable-Leave Timer, page 22-6
- IGMP Report Suppression, page 22-6
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 on an IGMPv2 switch and the switch receives an IGMPv3 report from a host, the switch can forward the IGMPv3 report to the multicast router.

Note

The switch supports IGMPv3 snooping based only on the destination multicast MAC address. It does not support snooping based on the source MAC address or on proxy reports.

An IGMPv3 switch supports Basic IGMPv3 Snooping Support (BISS), which includes support for the snooping features on IGMPv1 and IGMPv2 switches and for IGMPv3 membership report messages. BISS constrains the flooding of multicast traffic when your network includes IGMPv3 hosts. It constrains traffic to approximately the same set of ports as the IGMP snooping feature on IGMPv2 or IGMPv1 hosts.

Note

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

An IGMPv3 switch can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature. For more information about source-specific multicast with IGMPv3 and IGMP:

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dtssm5t.html

Joining a Multicast Group

When a host connected to the switch wants to join an IP multicast group and it is an IGMP Version 2 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. IGMP Version 1 or Version 2 hosts wanting to join the multicast group respond by sending a join message to the switch. The switch CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group. See Figure 22-1.
Router A sends a general query to the switch, which forwards the query to ports 2 through 5, which are all 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, as shown in Table 22-1, that includes the port numbers connected to Host 1 and the router.

**Table 22-1**  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 (Figure 22-2), the CPU receives that message and adds the port number of Host 4 to the forwarding table as shown in Table 22-2. Note that 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.
Understanding IGMP Snooping

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 wishes 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**

Immediate Leave is only supported on IGMP Version 2 hosts.

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.

**Note**

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

For configuration steps, see the “Enabling IGMP Immediate Leave” section on page 22-11.

**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 5000 milliseconds. The timer can be set either globally or on a per-VLAN basis. The VLAN configuration of the leave time overrides the global configuration.

For configuration steps, see the “Configuring the IGMP Leave Timer” section on page 22-11.

**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 router 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. For configuration steps, see the “Disabling IGMP Report Suppression” section on page 22-16.
Configuring IGMP Snooping

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. These sections contain this configuration information:

- Default IGMP Snooping Configuration, page 22-7
- Enabling or Disabling IGMP Snooping, page 22-7
- Setting the Snooping Method, page 22-8
- Configuring a Multicast Router Port, page 22-9
- Configuring a Host Statically to Join a Group, page 22-10
- Enabling IGMP Immediate Leave, page 22-11
- Configuring the IGMP Leave Timer, page 22-11
- Configuring TCN-Related Commands, page 22-12
- Configuring the IGMP Snooping Querier, page 22-14
- Disabling IGMP Report Suppression, page 22-16

Default IGMP Snooping Configuration

Table 22-3 shows the 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>Multicast router learning (snooping) method</td>
<td>PIM-DVMRP</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 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. TCN = Topology Change Notification

Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the switch. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. IGMP snooping is by default enabled on all VLANs, 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.
Chapter 22  Configuring IGMP Snooping and MVR

Configuring IGMP Snooping

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping Globally enable IGMP snooping in all existing VLAN interfaces.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To globally disable IGMP snooping on all VLAN interfaces, use the no ip igmp snooping global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping on a VLAN interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping vlan vlan-id Enable IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094. Note IGMP snooping must be globally enabled before you can enable VLAN snooping.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable IGMP snooping on a VLAN interface, use the no ip igmp snooping vlan vlan-id global configuration command for the specified VLAN number.

Setting the Snooping Method

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

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

You can configure the switch either to snoop on IGMP queries and PIM/DVMRP packets or to listen to CGMP self-join or proxy-join packets. By default, the switch snoops on PIM/DVMRP packets on all VLANs. To learn of multicast router ports through only CGMP packets, use the ip igmp snooping vlan vlan-id mrouter learn cgmp global configuration command. When this command is entered, the router listens to only CGMP self-join and CGMP proxy-join packets and to no other CGMP packets. To learn of multicast router ports through only PIM-DVMRP packets, use the ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp global configuration command.
Chapter 22  Configuring IGMP Snooping and MVR

Configuring IGMP Snooping

Note
If you want to use CGMP as the learning method and no multicast routers in the VLAN are CGMP proxy-enabled, you must enter the `ip cgmp router-only` command to dynamically access the router. For more information, see Chapter 45, “Configuring IP Multicast Routing.”

Beginning in privileged EXEC mode, follow these steps to alter the method in which a VLAN interface dynamically accesses a multicast router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping vlan (\text{vlan-id} ) mrouter learn {cgmp</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default learning method, use the `no ip igmp snooping vlan \(\text{vlan-id} \) mrouter learn cgmp` global configuration command.

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

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

Configuring a Multicast Router Port

To add a multicast router port (add a static connection to a multicast router), use the `ip igmp snooping vlan mrouter` global configuration command on the switch.

Note
Static connections to multicast routers are supported only on switch ports.
Beginning in privileged EXEC mode, follow these steps to enable a static connection to a multicast router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping vlan <code>vlan-id</code> mrouter interface <code>interface-id</code></td>
<td>Specify the multicast router VLAN ID and the interface to the multicast router:</td>
</tr>
<tr>
<td></td>
<td>• The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• The interface can be a physical interface or a port channel.</td>
</tr>
<tr>
<td></td>
<td>• The port-channel range is 1 to 48.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show ip igmp snooping mrouter [vlan <code>vlan-id</code>]</td>
<td>Verify that IGMP snooping is enabled on the VLAN interface.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove a multicast router port from the VLAN, use the `no ip igmp snooping vlan `vlan-id` mrouter interface `interface-id` global configuration command.

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

```bash
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config)# end
```

### Configuring a Host Statistically 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.

Beginning in privileged EXEC mode, follow these steps to add a Layer 2 port as a member of a multicast group:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping vlan <code>vlan-id</code> static <code>ip_address</code> interface <code>interface-id</code></td>
<td>Statically configure a Layer 2 port as a member of a multicast group:</td>
</tr>
<tr>
<td></td>
<td>• <code>vlan-id</code> is the multicast group VLAN ID. The range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td></td>
<td>• <code>ip-address</code> is the group IP address.</td>
</tr>
<tr>
<td></td>
<td>• <code>interface-id</code> is the member port. It can be a physical interface or a port channel (1 to 48).</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show ip igmp snooping groups</td>
<td>Verify the member port and the IP address.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet0/1
Switch(config)# end
```

### 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 only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN.

**Note**

Immediate Leave is supported only on IGMP Version 2 hosts.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping vlan vlan-id immediate-leave</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip igmp snooping vlan vlan-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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

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
```

### Configuring the IGMP Leave Timer

Follows these guidelines when configuring the IGMP leave timer:

- You can configure the leave time globally or on a per-VLAN basis.
- Configuring the leave time on a VLAN overrides the global setting.
- The default leave time is 1000 milliseconds.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2.
- 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.
Beginning in privileged EXEC mode, follow these steps to enable the IGMP configurable-leave timer:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp snooping last-member-query-interval time</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp snooping vlan vlan-id last-member-query-interval time</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp snooping</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To globally reset the IGMP leave timer to the default setting, use the `no ip igmp snooping last-member-query-interval` global configuration command.

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.

**Configuring TCN-Related Commands**

These sections describe how to control flooded multicast traffic during a TCN event:

- Controlling the Multicast Flooding Time After a TCN Event, page 22-12
- Recovering from Flood Mode, page 22-13
- Disabling Multicast Flooding During a TCN Event, page 22-13

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

You can control the time that multicast traffic is flooded after a TCN event by using the `ip igmp snooping tcn flood query count` global configuration command. This command configures the number of general queries for which multicast data traffic is flooded after a TCN event. Some examples of TCN events are when the client changed its location and the receiver is on same port that was blocked but is now forwarding, and when a port went down without sending a leave message.

If you set the TCN flood query count to 1 by using the `ip igmp snooping tcn flood query count` command, the flooding stops after receiving 1 general query. If you set the count to 7, the flooding until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.
Beginning in privileged EXEC mode, follow these steps to configure the TCN flood query count:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping tcn flood query count count</td>
<td>Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10. By default, the flooding query count is 2.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show ip igmp snooping</td>
<td>Verify the TCN settings.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default flooding query count, use the `no ip igmp snooping tcn flood query count` global configuration command.

**Recovering from Flood Mode**

When a topology change occurs, the spanning-tree root sends a special IGMP leave message (also known as global leave) with the group multicast address 0.0.0.0. However, when you enable the `ip igmp snooping tcn query solicit` global configuration command, the switch sends the global leave message whether or not it is the spanning-tree root. When the router receives this special leave, it immediately sends general queries, which expedite the process of recovering from the flood mode during the TCN event. Leaves are always sent if the switch is the spanning-tree root regardless of this configuration command. By default, query solicitation is disabled.

Beginning in privileged EXEC mode, follow these steps to enable the switch to send the global leave message whether or not it is the spanning-tree root:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping tcn query solicit</td>
<td>Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event. By default, query solicitation is disabled.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show ip igmp snooping</td>
<td>Verify the TCN settings.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default query solicitation, use the `no ip igmp snooping tcn query solicit` global configuration command.

**Disabling Multicast Flooding During a TCN Event**

When the switch receives a TCN, multicast traffic is flooded to all the ports until 2 general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding might exceed the capacity of the link and cause packet loss. You can use the `ip igmp snooping tcn flood` interface configuration command to control this behavior.
Beginning in privileged EXEC mode, follow these steps to disable multicast flooding on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 no ip igmp snooping tcn flood</td>
<td>Disable the flooding of multicast traffic during a spanning-tree TCN event.</td>
</tr>
<tr>
<td></td>
<td>By default, multicast flooding is enabled on an interface.</td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show ip igmp snooping</td>
<td>Verify the TCN settings.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To re-enable multicast flooding on an interface, use the **ip igmp snooping tcn flood** interface configuration command.

### Configuring the IGMP Snooping Querier

Follow these guidelines when configuring the IGMP snooping querier:

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

Beginning in privileged EXEC mode, follow these steps to enable the IGMP snooping querier feature in a VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip igmp snooping querier</td>
<td>Enable the IGMP snooping querier.</td>
</tr>
</tbody>
</table>
### Configuring IGMP Snooping

#### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>ip igmp snooping querier address &lt;ip_address&gt;</td>
<td>(Optional) Specify an IP address for the IGMP snooping querier. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier. <strong>Note</strong> The IGMP snooping querier does not generate an IGMP general query if it cannot find an IP address on the switch.</td>
</tr>
<tr>
<td>4</td>
<td>ip igmp snooping querier query-interval &lt;interval-count&gt;</td>
<td>(Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds.</td>
</tr>
<tr>
<td>5</td>
<td>ip igmp snooping querier tcn query [count &lt;count&gt;</td>
<td>interval &lt;interval&gt;]</td>
</tr>
<tr>
<td>6</td>
<td>ip igmp snooping querier timer expiry &lt;timeout&gt;</td>
<td>(Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds.</td>
</tr>
<tr>
<td>7</td>
<td>ip igmp snooping querier version &lt;version&gt;</td>
<td>(Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2.</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>9</td>
<td>show ip igmp snooping vlan &lt;vlan-id&gt;</td>
<td>(Optional) Verify that the IGMP snooping querier is enabled on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
<tr>
<td>10</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

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

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

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
Disabling 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.

IGMP report suppression is enabled by default. When it is enabled, the switch forwards only one IGMP report per multicast router query. When report suppression is disabled, all IGMP reports are forwarded to the multicast routers.

Beginning in privileged EXEC mode, follow these steps to disable IGMP report suppression:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>no ip igmp snooping report-suppression</td>
<td>Disable IGMP report suppression.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip igmp snooping</td>
<td>Verify that IGMP report suppression is disabled.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

Displaying 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.

To display IGMP snooping information, use one or more of the privileged EXEC commands in Table 22-4.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp snooping [vlan vlan-id]</td>
<td>Display the snooping configuration information for all VLANs on the switch or for a specified VLAN. (Optional) Enter <code>vlan vlan-id</code> to display information for a single VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.</td>
</tr>
</tbody>
</table>
| show ip igmp snooping groups [count |dynamic [count] | user [count]] | Display multicast table information for the switch or about a specific parameter:  
  - `count`—Display the total number of entries for the specified command options instead of the actual entries.  
  - `dynamic`—Display entries learned through IGMP snooping.  
  - `user`—Display only the user-configured multicast entries. |
Displaying IGMP Snooping Information

For more information about the keywords and options in these commands, see the command reference for this release.
Understanding Multicast VLAN Registration

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

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

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

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

- In compatible mode, multicast data received by MVR hosts is forwarded to all MVR data ports, regardless of MVR host membership on those ports. The multicast data is forwarded only to those receiver ports that MVR hosts have joined, either by IGMP reports or by MVR static configuration. IGMP reports received from MVR hosts are never forwarded from MVR data ports that were configured in the switch.

- In dynamic mode, multicast data received by MVR hosts on the switch is forwarded from only those MVR data and client ports that the MVR hosts have joined, either by IGMP reports or by MVR static configuration. Any IGMP reports received from MVR hosts are also forwarded from all the MVR data ports in the switch. This eliminates using unnecessary bandwidth on MVR data port links, which occurs when the switch runs in compatible mode.

Only Layer 2 ports take part in MVR. You must configure ports as MVR receiver ports. Only one MVR multicast VLAN per switch is supported.

Using MVR in a Multicast Television Application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. Figure 22-3 is an example configuration. DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to Switch A to join the appropriate multicast. If the IGMP report matches one of the configured IP multicast group addresses, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.
When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The switch CPU sends a MAC-based general query through the receiver port VLAN. If there is another set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time specified in the query. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency. Enable the Immediate-Leave feature only on receiver ports to which a single receiver device is connected.

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

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

Configuring MVR

These sections contain this configuration information:

- Default MVR Configuration, page 22-20
- MVR Configuration Guidelines and Limitations, page 22-20
- Configuring MVR Global Parameters, page 22-21
- Configuring MVR Interfaces, page 22-22

Default MVR Configuration

Table 22-5 shows the default MVR configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVR</td>
<td>Disabled globally and per interface</td>
</tr>
<tr>
<td>Multicast addresses</td>
<td>None configured</td>
</tr>
<tr>
<td>Query response time</td>
<td>0.5 second</td>
</tr>
<tr>
<td>Multicast VLAN</td>
<td>VLAN 1</td>
</tr>
<tr>
<td>Mode</td>
<td>Compatible</td>
</tr>
<tr>
<td>Interface (per port)</td>
<td>Neither a receiver nor a source port</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>Disabled on all ports</td>
</tr>
</tbody>
</table>

MVR Configuration Guidelines and Limitations

Follow these guidelines when configuring MVR:

- Receiver ports can only be access ports; they cannot be trunk ports. Receiver ports on a switch can be in different VLANs, but should not belong to the multicast VLAN.
- The maximum number of multicast entries (MVR group addresses) that can be configured on a switch (that is, the maximum number of television channels that can be received) is 256.
- MVR multicast data received in the source VLAN and leaving from receiver ports has its time-to-live (TTL) decremented by 1 in the switch.
• Because MVR on the switch uses IP multicast addresses instead of MAC multicast addresses, aliased IP multicast addresses are allowed on the switch. However, if the switch is interoperating with Catalyst 3550 or Catalyst 3500 XL switches, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).

• Do not configure MVR on private VLAN ports.

• MVR is not supported when multicast routing is enabled on a switch. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled, and you receive a warning message. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled, and you receive an error message.

• MVR can coexist with IGMP snooping on a switch.

• MVR data received on an MVR receiver port is not forwarded to MVR source ports.

• MVR does not support IGMPv3 messages.

### Configuring MVR Global Parameters

You do not need to set the optional MVR parameters if you choose to use the default settings. If you do want to change the default parameters (except for the MVR VLAN), you must first enable MVR.

**Note** For complete syntax and usage information for the commands used in this section, see the command reference for this release.

Beginning in privileged EXEC mode, follow these steps to configure MVR parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mvr</td>
<td>Enable MVR on the switch.</td>
</tr>
<tr>
<td>Step 3 mvr group ip-address [count]</td>
<td>Configure an IP multicast address on the switch or use the count parameter to configure a contiguous series of MVR group addresses (the range for count is 1 to 256; the default is 1). Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address. Each multicast address would correspond to one television channel.</td>
</tr>
<tr>
<td>Step 4 mvr querytime value</td>
<td>(Optional) Define the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The range is 1 to 100, and the default is 5 tenths or one-half second.</td>
</tr>
<tr>
<td>Step 5 mvr vlan vlan-id</td>
<td>(Optional) Specify the VLAN in which multicast data is received; all source ports must belong to this VLAN. The VLAN range is 1 to 1001 and 1006 to 4094. The default is VLAN 1.</td>
</tr>
<tr>
<td>Step 6 mvr mode {dynamic</td>
<td>compatible}</td>
</tr>
<tr>
<td></td>
<td>dynamic—Allows dynamic MVR membership on source ports.</td>
</tr>
<tr>
<td></td>
<td>compatible—Is compatible with Catalyst 3500 XL and Catalyst 2900 XL switches and does not support IGMP dynamic joins on source ports. The default is compatible mode.</td>
</tr>
</tbody>
</table>
Chapter 22  Configuring IGMP Snooping and MVR

Configuring MVR

To return the switch to its default settings, use the `no mvr [mode | group ip-address | querytime | vlan]` global configuration commands.

This example shows how to enable MVR, configure the group address, set the query time to 1 second (10 tenths), specify the MVR multicast VLAN as VLAN 22, and set the MVR mode as dynamic:

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(config)# end
```

You can use the `show mvr members` privileged EXEC command to verify the MVR multicast group addresses on the switch.

Configuring MVR Interfaces

Beginning in privileged EXEC mode, follow these steps to configure Layer 2 MVR interfaces:

<table>
<thead>
<tr>
<th>Command</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> mvr</td>
<td>Enable MVR on the switch.</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specify the Layer 2 port to configure, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 4** mvr type {source | receiver} | Configure an MVR port as one of these:  
  - source—Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN.  
  - receiver—Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.  

The default configuration is as a non-MVR port. If you attempt to configure a non-MVR port with MVR characteristics, the operation fails.
## Chapter 22 Configuring IGMP Snooping and MVR

### Configuring MVR

To return the interface to its default settings, use the **no mvr [type | immediate | vlan vlan-id | group]** interface configuration commands.

This example shows how to configure a port as a receiver port, statically configure the port to receive multicast traffic sent to the multicast group address, configure Immediate Leave on the port, and verify the results.

```plaintext
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config-if)# end
Switch# show mvr interface
Port  Type   Status       Immediate Leave
     ----  ------       ---------------
G10/2  RECEIVER   ACTIVE/DOWN  ENABLED
```

### Command Table

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>mvr vlan vlan-id group [ip-address]</td>
<td>(Optional) Statically configure a port to receive multicast traffic sent to the multicast VLAN and the IP multicast address. A port statically configured as a member of a group remains a member of the group until statically removed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> In compatible mode, this command applies to only receiver ports. In dynamic mode, it applies to receiver ports and source ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receiver ports can also dynamically join multicast groups by using IGMP join and leave messages.</td>
</tr>
<tr>
<td>6</td>
<td>mvr immediate</td>
<td>(Optional) Enable the Immediate-Leave feature of MVR on the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This command applies to only receiver ports and should only be enabled on receiver ports to which a single receiver device is connected.</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td>show mvr</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td></td>
<td>show mvr interface or show mvr members</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return the interface to its default settings, use the **no mvr [type | immediate | vlan vlan-id | group]** interface configuration commands.

This example shows how to configure a port as a receiver port, statically configure the port to receive multicast traffic sent to the multicast group address, configure Immediate Leave on the port, and verify the results.
Displaying MVR Information

You can display MVR information for the switch or for a specified interface. Beginning in privileged EXEC mode, use the commands in Table 22-6 to display MVR configuration:

<table>
<thead>
<tr>
<th>Table 22-6</th>
<th>Commands for Displaying MVR Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>show mvr</td>
<td>Displays MVR status and values for the switch—whether MVR is enabled or disabled, the multicast VLAN, the maximum (256) and current (0 through 256) number of multicast groups, the query response time, and the MVR mode.</td>
</tr>
</tbody>
</table>
| show mvr interface [interface-id] [members [vlan vlan-id]] | Displays all MVR interfaces and their MVR configurations. When a specific interface is entered, displays this information:  
  • Type—Receiver or Source  
  • Status—One of these:  
    – Active means the port is part of a VLAN.  
    – Up/Down means that the port is forwarding or nonforwarding.  
    – Inactive means that the port is not part of any VLAN.  
  • Immediate Leave—Enabled or Disabled  
If the members keyword is entered, displays all multicast group members on this port or, if a VLAN identification is entered, all multicast group members on the VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094. |
| show mvr members [ip-address] | Displays all receiver and source ports that are members of any IP multicast group or the specified IP multicast group IP address. |
Configuring IGMP Filtering and Throttling

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

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

IGMP filtering controls only group-specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP or MVR is used to forward the multicast traffic.

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

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

**Note**

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

These sections contain this configuration information:

- Default IGMP Filtering and Throttling Configuration, page 22-26
- Configuring IGMP Profiles, page 22-26 (optional)
- Applying IGMP Profiles, page 22-27 (optional)
- Setting the Maximum Number of IGMP Groups, page 22-28 (optional)
- Configuring the IGMP Throttling Action, page 22-29 (optional)
Default IGMP Filtering and Throttling Configuration

Table 22-7 shows the default IGMP filtering configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP filters</td>
<td>None applied</td>
</tr>
<tr>
<td>IGMP maximum number of IGMP groups</td>
<td>No maximum set</td>
</tr>
<tr>
<td>IGMP profiles</td>
<td>None defined</td>
</tr>
<tr>
<td>IGMP profile action</td>
<td>Deny the range addresses</td>
</tr>
</tbody>
</table>

When the maximum number of groups is in forwarding table, the default IGMP throttling action is to deny the IGMP report. For configuration guidelines, see the “Configuring the IGMP Throttling Action” section on page 22-29.

Configuring IGMP Profiles

To configure an IGMP profile, use the `ip igmp profile` global configuration command with a profile number to create an IGMP profile and to enter IGMP profile configuration mode. From this mode, you can specify the parameters of the IGMP profile to be used for filtering IGMP join requests from a port. When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: Specifies that matching addresses are denied; this is the default.
- **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. When a profile is configured, if neither the `permit` nor `deny` keyword is included, the default is to deny access to the range of IP addresses.
Beginning in privileged EXEC mode, follow these steps to create an IGMP profile:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp profile profile number</td>
</tr>
<tr>
<td>Step 3</td>
<td>permit</td>
</tr>
<tr>
<td></td>
<td>deny</td>
</tr>
<tr>
<td>Step 4</td>
<td>range ip multicast address</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip igmp profile profile number</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To delete a profile, use the `no ip igmp profile profile number` global configuration command.

To delete an IP multicast address or range of IP multicast addresses, use the `no range ip multicast address` IGMP profile configuration command.

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
```

### Applying IGMP Profiles

To control access as defined in an IGMP profile, use the `ip igmp filter` interface configuration command 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.
Beginning in privileged EXEC mode, follow these steps to apply an IGMP profile to a switch port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the physical interface, and enter interface configuration mode. The interface must be a Layer 2 port that does not belong to an EtherChannel port group.</td>
</tr>
<tr>
<td>Step 3 ip igmp filter profile number</td>
<td>Apply the specified IGMP profile to the interface. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config interface interface-id</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove a profile from an interface, use the no ip igmp filter profile number interface configuration command.

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
```

### Setting the Maximum Number of IGMP Groups

You can set the maximum number of IGMP groups that a Layer 2 interface can join by using the **ip igmp max-groups** interface configuration command. Use the **no** form of this command to set the maximum back to the default, which is no limit.

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.

Beginning in privileged EXEC mode, follow these steps to set the maximum number of IGMP groups in the forwarding table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode. The interface can be a Layer 2 port that does not belong to an EtherChannel group or a EtherChannel interface.</td>
</tr>
<tr>
<td>Step 3 ip igmp max-groups number</td>
<td>Set the maximum number of IGMP groups that the interface can join. The range is 0 to 4294967294. The default is to have no maximum set.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config interface interface-id</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To remove the maximum group limitation and return to the default of no maximum, use the `no ip igmp max-groups` interface configuration command.

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
```

### 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 by using the `ip igmp max-groups action replace` interface configuration command. Use the `no` form of this command to return to the default, which is to drop the IGMP join report.

Follow these guidelines when configuring the IGMP throttling action:

- This restriction can be applied only to Layer 2 ports. You can use this 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:
  - If you configure the throttling action as `deny`, 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.
  - If you configure the throttling action as `replace`, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly selected entry with the received IGMP report.

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.

Beginning in privileged EXEC mode, follow these steps to configure the throttling action when the maximum number of entries is in the forwarding table:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the physical interface to be configured, and enter 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>3</td>
<td>ip igmp max-groups action {deny</td>
<td>replace}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>deny</code>—Drop the report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>replace</code>—Replace the existing group with the new group for which the IGMP report was received.</td>
</tr>
</tbody>
</table>
Displaying IGMP Filtering and Throttling Configuration

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. You can also display the IGMP throttling configuration for all interfaces on the switch or for a specified interface.

Use the privileged EXEC commands in Table 22-8 to display IGMP filtering and throttling configuration:

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

This chapter describes how to configure the port-based traffic control features on the Catalyst 3560 switch.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Configuring Storm Control, page 23-1
- Configuring Protected Ports, page 23-6
- Configuring Port Blocking, page 23-8
- Configuring Port Security, page 23-9
- Displaying Port-Based Traffic Control Settings, page 23-20

Configuring Storm Control

These sections contain this conceptual and configuration information:

- Understanding Storm Control, page 23-2
- Default Storm Control Configuration, page 23-3
- Configuring Storm Control and Threshold Levels, page 23-3
- Configuring Small-Frame Arrival Rate, page 23-5
Understanding 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.

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.

**Note**

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.

The graph in Figure 23-1 shows broadcast traffic patterns on an interface over a given period of time. The example can also be applied to multicast and unicast traffic. In this example, the 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.
Configuring Storm Control

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.

Note
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.

Default Storm Control Configuration

By default, unicast, broadcast, and multicast storm control are disabled on the switch interfaces; that is, the suppression level is 100 percent.

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.
Beginning in privileged EXEC mode, follow these steps to storm control and threshold levels:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>storm-control {broadcast</td>
</tr>
</tbody>
</table>

The keywords have these meanings:

- For **level**, specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00.

- (Optional) For **level-low**, specify the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00.

If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked.

- For **bps bps**, specify the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0.

- (Optional) For **bps-low**, specify the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0.

- For **pps pps**, specify the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0.

- (Optional) For **pps-low**, specify the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is **0.0 to 10000000000.0**.

For BPS and PPS settings, you can use metric suffixes such as k, m, and g for large number thresholds.

Step 4 | storm-control action {shutdown | trap} | Specify the action to be taken when a storm is detected. The default is to filter out the traffic and not to send traps. |

- Select the **shutdown** keyword to error-disable the port during a storm.
- Select the **trap** keyword to generate an SNMP trap when a storm is detected.

Step 5 | end | Return to privileged EXEC mode. |
Configuring Storm Control

To disable storm control, use the `no storm-control [broadcast | multicast | unicast] level` interface configuration command.

This example shows how to enable unicast storm control on a port with an 87-percent rising suppression level and a 65-percent falling suppression level:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable broadcast address storm control on a port to a level of 20 percent. When the broadcast traffic exceeds the configured level of 20 percent of the total available bandwidth of the port within the traffic-storm-control interval, the switch drops all broadcast traffic until the end of the traffic-storm-control interval:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

### Configuring Small-Frame Arrival Rate

Incoming VLAN-tagged packets smaller than 67 bytes are considered small frames. They are forwarded by the switch, but they do not cause the switch storm-control counters to increment. In Cisco IOS Release 12.2(44)SE and later, you can configure a port to be error disabled if small frames arrive at a specified rate (threshold).

You globally enable the small-frame arrival feature on the switch and then configure the small-frame threshold for packets on each interface. Packets smaller than the minimum size and arriving at a specified rate (the threshold) are dropped since the port is error disabled.

If the `errdisable recovery cause small-frame` global configuration command is entered, the port is re-enabled after a specified time. (You specify the recovery time by using `errdisable recovery` global configuration command.)

**Note**

Small Frame Arrival-Rate is supported by 3560 and 3560G.

### Command Purpose

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`show storm-control [interface-id] [broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to configure the threshold level for each interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>errdisable detect cause small-frame</td>
<td>Enable the small-frame rate-arrival feature on the switch.</td>
</tr>
<tr>
<td>3</td>
<td>errdisable recovery interval interval</td>
<td>(Optional) Specify the time to recover from the specified error-disabled state.</td>
</tr>
<tr>
<td>4</td>
<td>errdisable recovery cause small-frame</td>
<td>(Optional) Configure the recovery time for error-disabled ports to be automatically re-enabled after they are error disabled by the arrival of small frames.</td>
</tr>
<tr>
<td>5</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to be configured.</td>
</tr>
<tr>
<td>6</td>
<td>small violation-rate pps</td>
<td>Configure the threshold rate for the interface to drop incoming packets and error disable the port. The range is 1 to 10,000 packets per second (pps).</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td>show interfaces interface-id</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>9</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable the small-frame arrival-rate feature, configure the port recovery time, and configure the threshold for error disabling a port:

```
Switch# configure terminal
Switch# errdisable detect cause small-frame
Switch# errdisable recovery cause small-frame
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# small-frame violation rate 10000
Switch(config-if)# end
```

**Configuring 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.
These sections contain this configuration information:

- Default Protected Port Configuration, page 23-7
- Protected Port Configuration Guidelines, page 23-7
- Configuring a Protected Port, page 23-7

**Default Protected Port Configuration**

The default is to have no protected ports defined.

**Protected Port Configuration 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.

Do not configure a private-VLAN port as a protected port. Do not configure a protected port as a private-VLAN port. A private-VLAN isolated port does not forward traffic to other isolated ports or community ports. For more information about private VLANs, see Chapter 15, “Configuring Private VLANs.”

**Configuring a Protected Port**

Beginning in privileged EXEC mode, follow these steps to define a port as a protected port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 switchport protected</td>
<td>Configure the interface to be a protected port.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show interfaces interface-id switchport</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable protected port, use the `no switchport protected` interface configuration command.

This example shows how to configure a port as a protected port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport protected
Switch(config-if)# end
```
## Configuring 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.

**Note**  
With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

These sections contain this configuration information:

- Default Port Blocking Configuration, page 23-8
- Blocking Flooded Traffic on an Interface, page 23-8

### Default Port Blocking Configuration

The default is to not block flooding of unknown multicast and unicast traffic out of a port, but to flood these packets to all ports.

### Blocking Flooded Traffic on an Interface

**Note**  
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.

Beginning in privileged EXEC mode, follow these steps to disable the flooding of unicast packets and Layer 2 multicast packets out of an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>switchport block multicast</strong></td>
</tr>
<tr>
<td></td>
<td>Block unknown multicast forwarding out of the port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>switchport block unicast</strong></td>
</tr>
<tr>
<td></td>
<td>Block unknown unicast forwarding out of the port.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>show interfaces interface-id switchport</strong></td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To return the interface to the default condition where no traffic is blocked and normal forwarding occurs on the port, use the `no switchport block {multicast | unicast}` interface configuration commands.

This example shows how to block unicast and Layer 2 multicast flooding on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config-if)# end
```

## Configuring 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.

These sections contain this conceptual and configuration information:

- Understanding Port Security, page 23-9
- Default Port Security Configuration, page 23-11
- Port Security Configuration Guidelines, page 23-12
- Enabling and Configuring Port Security Aging, page 23-18
- Port Security and Private VLANs, page 23-19

## Understanding Port Security

These sections contain this conceptual information:

- Secure MAC Addresses, page 23-9
- Security Violations, page 23-10

## Secure MAC Addresses

You configure the maximum number of secure addresses allowed on a port by using the `switchport port-security maximum value` interface configuration command.

**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.
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.

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. To enable sticky learning, enter the `switchport port-security mac-address sticky` interface configuration command. When you enter this command, 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.

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 determined by the active Switch Database Management (SDM) template. See Chapter 7, “Configuring SDM Templates.” 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.

**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.

You can configure the interface for one of four 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 shutdown` 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.

Table 23-1 shows the violation mode and the actions taken when you configure an interface for port security.

### Table 23-1  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>Yes</td>
</tr>
<tr>
<td>shutdown</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</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>

1. Packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses.
2. The switch returns an error message if you manually configure an address that would cause a security violation.
3. Shuts down only the VLAN on which the violation occurred.

### Default Port Security Configuration

Table 23-2 shows the default port security configuration for an interface.

### Table 23-2  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

Follow these guidelines when configuring port security:

- 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).
- A secure port cannot belong to a Fast EtherChannel or a Gigabit EtherChannel port group.

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.

Table 23-3 summarizes port security compatibility with other port-based features.

<table>
<thead>
<tr>
<th>Type of Port or Feature on Port</th>
<th>Compatible with Port Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTP1 port2</td>
<td>No</td>
</tr>
<tr>
<td>Trunk port</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic-access port3</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>No</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 port4</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Enabling and Configuring Port Security

Beginning in privileged EXEC mode, follow these steps to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode (access</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport voice vlan vlan-id</td>
</tr>
<tr>
<td></td>
<td>vlan-id—Specify the VLAN to be used for voice traffic.</td>
</tr>
<tr>
<td>Step 5</td>
<td>switchport port-security</td>
</tr>
</tbody>
</table>
Step 6  

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `switchport port-security [maximum value [vlan {vlan-list | access | voice} ]]]` | (Optional) Set the maximum number of secure MAC addresses for the interface. 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 set by the active Switch Database Management (SDM) template. See Chapter 7, “Configuring the Switch SDM Template.” 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.  
(Optional) `vlan`—set 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, specify the VLAN as an access VLAN.  
- `voice`—On an access port, specify 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.
### Configuring Port Security

**Step 7**

**Command**

```
switchport port-security [violation {protect | restrict | shutdown | shutdown vlan}]
```

**Purpose**

(Optional) Set the violation mode, the action to be taken when a security violation is detected, as one of these:

- **protect**—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

  **Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

- **restrict**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- **shutdown**—The interface is error disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

- **shutdown vlan**—Use to set the security violation mode per VLAN. In this mode, the VLAN is error disabled instead of the entire port when a violation occurs.

  **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.
## Configuring Port Security

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport port-security</td>
<td>(Optional) Enter a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.</td>
<td></td>
</tr>
<tr>
<td>[mac-address mac-address [vlan [vlan-id</td>
<td>{access</td>
<td>voice}]]]</td>
</tr>
</tbody>
</table>

(Optional) **vlan**—set 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, specify the VLAN as an access VLAN.
- **voice**—On an access port, specify 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>switchport port-security</th>
<th>(Optional) Enable sticky learning on the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address sticky</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>switchport port-security</th>
<th>(Optional) Enter 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address sticky [mac-address</td>
<td>(Optional) <strong>vlan</strong>—set a per-VLAN maximum value.</td>
<td></td>
</tr>
</tbody>
</table>
| vlan [vlan-id | Enter one of these options after you enter the **vlan** keyword:
| {access | voice}]]] | 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. |

- **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, specify the VLAN as an access VLAN.
- **voice**—On an access port, specify 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.

<table>
<thead>
<tr>
<th>Step 11</th>
<th>end</th>
<th>Return to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 12</td>
<td>show port-security</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 13</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To return the interface to the default condition as not a secure port, use the `no switchport port-security` interface configuration command. If you enter this command when sticky learning is enabled, the sticky secure addresses remain part of the running configuration but are removed from the address table. All addresses are now dynamically learned.

To return the interface to the default number of secure MAC addresses, use the `no switchport port-security maximum value` interface configuration command. To return the violation mode to the default condition (shutdown mode), use the `no switchport port-security violation {protocol | restrict}` interface configuration command.

To disable sticky learning on an interface, use the `no switchport port-security mac-address sticky` interface configuration command. The interface converts the sticky secure MAC addresses to dynamic secure addresses. However, if you have previously saved the configuration with the sticky MAC addresses, you should save the configuration again after entering the `no switchport port-security mac-address sticky` command, or the sticky addresses will be restored if the switch reboots.

Use the `clear port-security {all | configured | dynamic | sticky}` privileged EXEC command to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

To delete a specific secure MAC address from the address table, use the `no switchport port-security mac-address mac-address` interface configuration command. To delete all dynamic secure addresses on an interface from the address table, enter the `no switchport port-security` interface configuration command followed by the `switchport port-security` command (to re-enable port security on the interface). If you use the `no switchport port-security mac-address sticky` interface configuration command to convert sticky secure MAC addresses to dynamic secure MAC addresses before entering the `no switchport port-security` command, all secure addresses on the interface except those that were manually configured are deleted.

You must specifically delete configured secure MAC addresses from the address table by using the `no switchport port-security mac-address mac-address` interface configuration command.

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 gigabitethernet0/1
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 gigabitethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 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 gigabitethernet0/1
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 mac-address 0000.0000.0002
```

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 vlan 3
```

```
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# switchport mode access
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 mac-address 0000.0000.0002
```

```
Switch(config)# interface gigabitethernet0/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 vlan 3
```

```
Switch(config)# interface gigabitethernet0/5
Switch(config-if)# switchport mode access
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 mac-address 0000.0000.0002
```

```
Switch(config)# interface gigabitethernet0/6
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 vlan 3
```

```
Switch(config)# interface gigabitethernet0/7
Switch(config-if)# switchport mode access
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 mac-address 0000.0000.0002
```

```
Switch(config)# interface gigabitethernet0/8
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 vlan 3
```

```
Switch(config)# interface gigabitethernet0/9
Switch(config-if)# switchport mode access
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 mac-address 0000.0000.0002
```

```
Switch(config)# interface gigabitethernet0/10
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 vlan 3
```

```
Switch(config)# interface gigabitethernet0/11
Switch(config-if)# switchport mode access
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 mac-address 0000.0000.0002
```

```
Switch(config)# interface gigabitethernet0/12
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 vlan 3
```

```
Switch(config)# interface gigabitethernet0/13
Switch(config-if)# switchport mode access
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 mac-address 0000.0000.0002
```

```
Switch(config)# interface gigabitethernet0/14
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address mac-address 0000.02000.0004 vlan 3
```

```
Switch(config)# interface gigabitethernet0/15
Switch(config-if)# switchport mode access
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 mac-address 0000.0000.0002
```
Enabling and Configuring 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.

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.

Beginning in privileged EXEC mode, follow these steps to configure port security aging:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>switchport port-security aging {static</td>
<td>time time time</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter <strong>static</strong> to enable aging for statically configured secure addresses on this port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For <strong>time</strong>, specify the aging time for this port. The valid range is from 0 to 1440 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For <strong>type</strong>, select one of these keywords:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>absolute</strong>—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>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>inactivity</strong>—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>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show port-security [interface interface-id] [address]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To disable port security aging for all secure addresses on a port, use the `no switchport port-security aging time` interface configuration command. To disable aging for only statically configured secure addresses, use the `no switchport port-security aging static` interface configuration command.

This example shows how to set the aging time as 2 hours for the secure addresses on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes for the inactivity aging type with aging enabled for the configured secure addresses on the interface:

```
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

You can verify the previous commands by entering the `show port-security interface interface-id` privileged EXEC command.

## Port Security and Private VLANs

Port security allows an administrator to limit the number of MAC addresses learned on a port or to define which MAC addresses can be learned on a port.

Beginning in privileged EXEC mode, follow these steps to configure port security on a PVLAN host and promiscuous ports:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>switchport mode private-vlan {host</td>
<td>promiscuous}</td>
</tr>
<tr>
<td>4</td>
<td>switchport port-security</td>
<td>Enable port security on the interface.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show port-security [interface interface-id] [address]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport private-vlan mapping 2061 2201-2206,3101
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport port-security maximum 288
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security violation restrict
```

**Note**

Ports that have both port security and private VLANs configured can be labeled secure PVLAN ports. When a secure address is learned on a secure PVLAN port, the same secure address cannot be learned on another secure PVLAN port belonging to the same primary VLAN. However, an address learned on unsecure PVLAN port can be learned on a secure PVLAN port belonging to same primary VLAN.
Secure addresses that are learned on host port get automatically replicated on associated primary VLANs, and similarly, secure addresses learned on promiscuous ports automatically get replicated on all associated secondary VLANs. Static addresses (using mac-address-table static command) cannot be user configured on a secure port.

Displaying Port-Based Traffic Control Settings

The `show interfaces interface-id switchport` privileged EXEC command displays (among other characteristics) the interface traffic suppression and control configuration. The `show storm-control` and `show port-security` privileged EXEC commands display those storm control and port security settings.

To display traffic control information, use one or more of the privileged EXEC commands in Table 23-4.

<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>
<tr>
<td>`show storm-control [interface-id] [broadcast</td>
<td>multicast</td>
</tr>
<tr>
<td><code>show port-security [interface interface-id]</code></td>
<td>Displays port security settings for the switch or for the specified interface, including the maximum allowed number of secure MAC addresses for each interface, the number of secure MAC addresses on the interface, the number of security violations that have occurred, and the violation mode.</td>
</tr>
<tr>
<td><code>show port-security [interface interface-id] address</code></td>
<td>Displays all secure MAC addresses configured on all switch interfaces or on a specified interface with aging information for each address.</td>
</tr>
<tr>
<td><code>show port-security interface interface-id vlan</code></td>
<td>Displays the number of secure MAC addresses configured per VLAN on the specified interface.</td>
</tr>
</tbody>
</table>
Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Catalyst 3560 switch.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the “System Management Commands” section in the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

This chapter consists of these sections:

- Understanding CDP, page 24-1
- Configuring CDP, page 24-2
- Monitoring and Maintaining CDP, page 24-5

Understanding CDP

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

On the switch, CDP enables Network Assistant to display a graphical view of the network. The switch uses CDP to find cluster candidates and maintain information about cluster members and other devices up to three cluster-enabled devices away from the command switch by default.
For a switch and connected endpoint devices running Cisco Medianet

- CDP 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.

For information, go to:

The switch supports CDP Version 2.

**Configuring CDP**

These sections contain this configuration information:

- Default CDP Configuration, page 24-2
- Configuring the CDP Characteristics, page 24-3
- Disabling and Enabling CDP, page 24-3
- Disabling and Enabling CDP on an Interface, page 24-4

**Default CDP Configuration**

Table 24-1 shows the default CDP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP global state</td>
<td>Enabled</td>
</tr>
<tr>
<td>CDP interface state</td>
<td>Enabled</td>
</tr>
<tr>
<td>CDP timer (packet update frequency)</td>
<td>60 seconds</td>
</tr>
<tr>
<td>CDP holdtime (before discarding)</td>
<td>180 seconds</td>
</tr>
<tr>
<td>CDP Version-2 advertisements</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Configuring the CDP Characteristics

You can configure the frequency of CDP updates, the amount of time to hold the information before discarding it, and whether or not to send Version-2 advertisements.

Beginning in privileged EXEC mode, follow these steps to configure the CDP timer, holdtime, and advertisement type.

**Note** Steps 2 through 4 are all optional and can be performed in any order.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>cdp timer <em>seconds</em></td>
<td>(Optional) Set the transmission frequency of CDP updates in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The range is 5 to 254; the default is 60 seconds.</td>
</tr>
<tr>
<td>3</td>
<td>cdp holdtime <em>seconds</em></td>
<td>(Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The range is 10 to 255 seconds; the default is 180 seconds.</td>
</tr>
<tr>
<td>4</td>
<td>cdp advertise-v2</td>
<td>(Optional) Configure CDP to send Version-2 advertisements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is the default state.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show cdp</td>
<td>Verify your settings.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no** form of the CDP commands to return to the default settings.

This example shows how to configure CDP characteristics.

```
Switch# configure terminal
Switch(config)# cdp timer 50
Switch(config)# cdp holdtime 120
Switch(config)# cdp advertise-v2
Switch(config)# end
```

For additional CDP **show** commands, see the “Monitoring and Maintaining CDP” section on page 24-5.

### Disabling and Enabling CDP

CDP is enabled by default.

**Note** Switch clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages. Disabling CDP can interrupt cluster discovery and device connectivity. For more information, see Chapter 5, “Clustering Switches” and see *Getting Started with Cisco Network Assistant*, available on Cisco.com.
Beginning in privileged EXEC mode, follow these steps to disable the CDP device discovery capability:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>no cdp run</td>
<td>Disable CDP.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to enable CDP when it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>cdp run</td>
<td>Enable CDP after disabling it.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This example shows how to enable CDP if it has been disabled.

```
Switch# configure terminal
Switch(config)# cdp run
Switch(config)# end
```

### Disabling and Enabling CDP on an Interface

CDP is enabled by default on all supported interfaces to send and to receive CDP information.

Beginning in privileged EXEC mode, follow these steps to disable CDP on a port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the interface on which you are disabling CDP, and enter</td>
</tr>
<tr>
<td></td>
<td>interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>no cdp enable</td>
<td>Disable CDP on the interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to enable CDP on a port when it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the interface on which you are enabling CDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td>cdp enable</td>
<td>Enable CDP on the interface after disabling it.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable CDP on a port when it has been disabled.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# cdp enable
Switch(config-if)# end
```

**Note**
Voice VLAN is not counted against port security when CDP is disabled on the switch interface.

## Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cdp counters</td>
<td>Reset the traffic counters to zero.</td>
</tr>
<tr>
<td>clear cdp table</td>
<td>Delete the CDP table of information about neighbors.</td>
</tr>
<tr>
<td>show cdp</td>
<td>Display global information, such as frequency of transmissions and the holdtime for packets being sent.</td>
</tr>
<tr>
<td>show cdp entry entry-name [protocol</td>
<td>version]</td>
</tr>
<tr>
<td>show cdp interface interface-id</td>
<td>Display information about interfaces where CDP is enabled. You can limit the display to the interface about which you want information.</td>
</tr>
</tbody>
</table>
Chapter 24      Configuring CDP

Monitoring and Maintaining CDP

show cdp neighbors [interface-id] [detail]

Display 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

Display CDP counters, including the number of packets sent and received and checksum errors.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cdp neighbors</td>
<td>Display information about neighbors, including device type, interface type</td>
</tr>
<tr>
<td>[interface-id]</td>
<td>and number, holdtime settings, capabilities, platform, and port ID.</td>
</tr>
<tr>
<td>[detail]</td>
<td>You can limit the display to neighbors of a specific interface or expand the</td>
</tr>
<tr>
<td></td>
<td>display to provide more detailed information.</td>
</tr>
<tr>
<td>show cdp traffic</td>
<td>Display CDP counters, including the number of packets sent and received and</td>
</tr>
<tr>
<td></td>
<td>checksum errors.</td>
</tr>
</tbody>
</table>
CHAPTER 25

Configuring LLDP, LLDP-MED, and Wired Location Service

This chapter describes how to configure the Link Layer Discovery Protocol (LLDP), LLDP Media Endpoint Discovery (LLDP-MED) and wired location service on the Catalyst 3560 switch.

Note: For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the “System Management Commands” section in the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2.

- Understanding LLDP, LLDP-MED, and Wired Location Service, page 25-1
- Configuring LLDP, LLDP-MED, and Wired Location Service, page 25-5
- Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service, page 25-12

Understanding 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, and switches). 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 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)

**Note**

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


**LLDP-MED**

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

LLDP-MED 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-signalling 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. However, it does not provide for power negotiation between the endpoint and the network connectivity devices.
Starting with Cisco IOS Release 12.2(52)SE, when 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 (15.4 W) 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 (15.4 W).

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

- **Location TLV**
  Provides location information from the switch to the endpoint device. The location TLV can send this information:
  - Civic location information
    Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.
  - ELIN location information
    Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

### Wired Location Service

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

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

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

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

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

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

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

If you change a location address on the switch, the switch sends an NMSP location notification message that identifies the affected ports and the changed address information.
Configuring LLDP, LLDP-MED, and Wired Location Service

- Default LLDP Configuration, page 25-5
- Configuration Guidelines, page 25-5
- Enabling LLDP, page 25-6
- Configuring LLDP Characteristics, page 25-7
- Configuring LLDP-MED TLVs, page 25-8
- Configuring Network-Policy TLV, page 25-9
- Configuring Location TLV and Wired Location Service, page 25-10

Default LLDP Configuration

Table 25-1 Default LLDP Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP global state</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP holdtime (before discarding)</td>
<td>120 seconds</td>
</tr>
<tr>
<td>LLDP timer (packet update frequency)</td>
<td>30 seconds</td>
</tr>
<tr>
<td>LLDP reinitialization delay</td>
<td>2 seconds</td>
</tr>
<tr>
<td>LLDP tlv-select</td>
<td>Disabled to send and receive all TLVs</td>
</tr>
<tr>
<td>LLDP interface state</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP receive</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP transmit</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP med-tlv-select</td>
<td>Disabled to send all LLDP-MED TLVs. When LLDP is globally enabled, LLDP-MED-TLV is also enabled.</td>
</tr>
</tbody>
</table>

Configuration Guidelines

- 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.
- You cannot configure a network-policy profile on a private-VLAN port.
- For wired location to function, you must first enter the `ip device tracking` global configuration command.
Enabling LLDP

Beginning in privileged EXEC mode, follow these steps to enable LLDP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 lldp run</td>
<td>Enable LLDP globally on the switch.</td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Specify the interface on which you are enabling LLDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 lldp transmit</td>
<td>Enable the interface to send LLDP packets.</td>
</tr>
<tr>
<td>Step 5 lldp receive</td>
<td>Enable the interface to receive LLDP packets.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show lldp</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable LLDP, use the no lldp run global configuration command. To disable LLDP on an interface, use the no lldp transmit and the no lldp receive interface configuration commands.

This example shows how to globally enable LLDP.

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)# end
```

This example shows how to enable LLDP on an interface.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
```
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.

Beginning in privileged EXEC mode, follow these steps to configure the LLDP characteristics.

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>lldp holdtime seconds</td>
<td>(Optional) Specify 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.</td>
</tr>
<tr>
<td>3</td>
<td>lldp reinit delay</td>
<td>(Optional) Specify the delay time in seconds for LLDP to initialize on an interface. The range is 2 to 5 seconds; the default is 2 seconds.</td>
</tr>
<tr>
<td>4</td>
<td>lldp timer rate</td>
<td>(Optional) Set the sending frequency of LLDP updates in seconds. The range is 5 to 65534 seconds; the default is 30 seconds.</td>
</tr>
<tr>
<td>5</td>
<td>lldp tlv-select</td>
<td>(Optional) Specify the LLDP TLVs to send or receive.</td>
</tr>
<tr>
<td>6</td>
<td>interface interface-id</td>
<td>Specify the interface on which you are enabling LLDP, and enter interface configuration mode.</td>
</tr>
<tr>
<td>7</td>
<td>lldp med-tlv-select</td>
<td>(Optional) Specify the LLDP-MED TLVs to send or receive.</td>
</tr>
<tr>
<td>8</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>9</td>
<td>show lldp</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>10</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no** form of each of the LLDP commands to return to the default setting.

This example shows how to configure LLDP characteristics.

```
Switch# configure terminal
Switch(config)# lldp holdtime 120
Switch(config)# lldp reinit 2
Switch(config)# lldp timer 30
Switch(config)# end
```

---

**Note:** Steps 2 through 5 are optional and can be performed in any order.
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 Table 25-2.

<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>

Beginning in privileged EXEC mode, follow these steps to enable a TLV on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface on which you are configuring an LLDP-MED TLV, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 lldp med-tlv-select tlv</td>
<td>Specify the TLV to enable.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable a TLV on an interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lldp med-tlv-select inventory-management
Switch(config-if)# end
```
Configuring Network-Policy TLV

Beginning in privileged EXEC mode, follow these steps to create a network-policy profile, configure the policy attributes, and apply it to an interface.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>network-policy profile profile number</td>
<td>Specify the network-policy profile number, and enter network-policy configuration mode. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>Step 3</td>
<td>{ voice</td>
<td>voice-signaling } vlan [vlan-id {cos cvalue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>voice—Specify the voice application type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>voice-signaling—Specify the voice-signaling application type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan—Specify the native VLAN for voice traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vlan-id—(Optional) Specify the VLAN for voice traffic. The range is 1 to 4094.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cos cvalue—(Optional) Specify the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dscp dvalue—(Optional) Specify the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dot1p—(Optional) Configure the telephone to use IEEE 802.1p priority tagging and use VLAN 0 (the native VLAN).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none—(Optional) Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>untagged—(Optional) Configure the telephone to send untagged voice traffic. This is the default for the telephone.</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>interface interface-id</td>
<td>Specify the interface on which you are configuring a network-policy profile, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>network-policy profile number</td>
<td>Specify the network-policy profile number.</td>
</tr>
<tr>
<td>Step 7</td>
<td>lldp med-tlv-select network-policy</td>
<td>Specify the network-policy TLV.</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 9</td>
<td>show network-policy profile</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no form of each command to return to the default setting.
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 gigabitethernet0/1
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

Configuring Location TLV and Wired Location Service

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>location {admin-tag string</td>
<td>civic-location identifier id</td>
</tr>
<tr>
<td></td>
<td>• admin-tag—Specify an administrative tag or site information.</td>
</tr>
<tr>
<td></td>
<td>• civic-location—Specify civic location information.</td>
</tr>
<tr>
<td></td>
<td>• elin-location—Specify emergency location information (ELIN).</td>
</tr>
<tr>
<td></td>
<td>• identifier id—Specify the ID for the civic location.</td>
</tr>
<tr>
<td></td>
<td>• string—Specify the site or location information in alphanumeric format.</td>
</tr>
<tr>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the interface on which you are configuring the location information, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| location {additional-location-information word | civic-location-id id | elin-location-id id} | Enter location information for an interface:
|                                                                         | additional-location-information—Specify additional information for a location or place. |
|                                                                         | civic-location-id—Specify global civic location information for an interface. |
|                                                                         | elin-location-id—Specify emergency location information for an interface. |
|                                                                         | id—Specify the ID for the civic location or the ELIN location. The ID range is 1 to 4095. |
|                                                                         | word—Specify a word or phrase with additional location information. |
| end                                                                    | Return to privileged EXEC mode.              |
### Configuring LLDP, LLDP-MED, and Wired Location Service

#### Chapter 25  
**Configuring LLDP, LLDP-MED, and Wired Location Service**

Use the **no** form of each command to return to the default setting.

This example shows how to configure civic location information on the switch:

```plaintext
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

Beginning in privileged EXEC mode, follow these steps to enable wired location service on the switch.

**Note**  
Your switch must be running the cryptographic (encrypted) software image to enable the `nmsp` global configuration commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>nmsp enable</code></td>
<td>Enable the NMSP features on the switch.</td>
</tr>
<tr>
<td>`nmsp notification interval [attachment</td>
<td>Specify the NMSP notification interval.</td>
</tr>
<tr>
<td>location] interval-seconds`</td>
<td><code>attachment</code>—Specify the attachment notification interval.</td>
</tr>
<tr>
<td></td>
<td><code>location</code>—Specify the location notification interval.</td>
</tr>
<tr>
<td></td>
<td><code>interval-seconds</code>—Duration in seconds before the switch sends the MSE the location or attachment updates. The range is 1 to 30; the default is 30.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show network-policy profile</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to enable NMSP on a switch and to set the location notification time to 10 seconds:

```plaintext
Switch(config)# nmsp enable
Switch(config)# nmsp notification interval location 10
```
## Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service

To monitor and maintain LLDP, LLDP-MED, and wired location service on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear lldp counters</td>
<td>Reset the traffic counters to zero.</td>
</tr>
<tr>
<td>clear lldp table</td>
<td>Delete the LLDP neighbor information table.</td>
</tr>
<tr>
<td>clear nmsp statistics</td>
<td>Clear the NMSP statistic counters.</td>
</tr>
<tr>
<td>show lldp</td>
<td>Display 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>Display information about a specific neighbor. You can enter an asterisk (*) to display all neighbors, or you can enter the neighbor name.</td>
</tr>
<tr>
<td>show lldp interface [interface-id]</td>
<td>Display information about interfaces with LLDP enabled. You can limit the display to a specific interface.</td>
</tr>
<tr>
<td>show lldp neighbors [interface-id] [detail]</td>
<td>Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID. You can limit the display to neighbors of a specific interface or expand the display for more detailed information.</td>
</tr>
<tr>
<td>show lldp traffic</td>
<td>Display LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.</td>
</tr>
<tr>
<td>show location</td>
<td>Display the location information for an endpoint.</td>
</tr>
<tr>
<td>show network-policy profile</td>
<td>Display the configured network-policy profiles.</td>
</tr>
<tr>
<td>show nmsp</td>
<td>Display the NMSP information.</td>
</tr>
</tbody>
</table>
Configuring UDLD

This chapter describes how to configure the UniDirectional Link Detection (UDLD) protocol on the Catalyst 3560 switch.

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding UDLD, page 27-1
- Configuring UDLD, page 27-3
- Displaying UDLD Status, page 27-6

Understanding UDLD

UDLD is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected ports on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected ports on fiber-optic links.

In normal and aggressive modes, UDLD works with the Layer 1 mechanisms to learn the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.
Understanding UDLD

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic port are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the ports are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In this case, the logical link is considered undetermined, and UDLD does not disable the port.

When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected, as long as autonegotiation is active, the link does not stay up because the Layer 1 mechanisms detects a physical problem with the link. In this case, UDLD does not take any action and the logical link is considered undetermined.

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 re-establish 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.

Methods to Detect Unidirectional Links

UDLD operates by using two mechanisms:

- 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 mechanism. 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.

If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined.

Figure 27-1 shows an example of a unidirectional link condition.

**Figure 27-1  UDLD Detection of a Unidirectional Link**

Switch B successfully receives traffic from Switch A on this port. However, Switch A does not receive traffic from Switch B on the same port. If UDLD is in aggressive mode, it detects the problem and disables the port. If UDLD is in normal mode, the logical link is considered undetermined, and UDLD does not disable the interface.

---

**Configuring UDLD**

These sections contain this configuration information:

- Default UDLD Configuration, page 27-4
- Configuration Guidelines, page 27-4
- Enabling UDLD Globally, page 27-5
- Enabling UDLD on an Interface, page 27-5
- Resetting an Interface Disabled by UDLD, page 27-6
Default UDLD Configuration

Table 27-1 shows the default UDLD configuration.

Table 27-1  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>

Configuration Guidelines

These are the UDLD configuration guidelines:

- UDLD is not supported on ATM ports.
- 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.
Enabling UDLD Globally

Beginning in privileged EXEC mode, 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>udld {aggressive</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• aggressive—Enables UDLD in aggressive mode on all fiber-optic ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• enable—Enables UDLD in normal mode on all fiber-optic ports on the switch. UDLD is disabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An individual interface configuration overrides the setting of the udld enable global configuration command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about aggressive and normal modes, see the “Modes of Operation” section on page 27-1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• message time message-timer-interval—Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. The range is from 1 to 90 seconds. The default value is 15.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This command affects fiber-optic ports only. Use the udld interface configuration command to enable UDLD on other port types. For more information, see the “Enabling UDLD on an Interface” section on page 27-5.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show udl</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable UDLD globally, use the **no udld enable** global configuration command to disable normal mode UDLD on all fiber-optic ports. Use the **no udld aggressive** global configuration command to disable aggressive mode UDLD on all fiber-optic ports.

Enabling UDLD on an Interface

Beginning in privileged EXEC mode, follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the port to be enabled for UDLD, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
### Displaying UDLD Status

To display the UDLD status for the specified port or for all ports, use the `show udld [interface-id]` privileged EXEC command.

For detailed information about the fields in the command output, see the command reference for this release.
Configuring SPAN and RSPAN

This chapter describes how to configure Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) on the Catalyst 3560 switch.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:
- Understanding SPAN and RSPAN, page 28-1
- Configuring SPAN and RSPAN, page 28-9
- Displaying SPAN and RSPAN Status, page 28-23

Understanding SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN 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 or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

You can use the SPAN or RSPAN 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.
Understanding SPAN and RSPAN

These sections contain this conceptual information:

- Local SPAN, page 28-2
- Remote SPAN, page 28-2
- SPAN and RSPAN Concepts and Terminology, page 28-3
- SPAN and RSPAN Interaction with Other Features, page 28-8

Local SPAN

Local SPAN supports a SPAN session entirely within one switch; all source ports or source VLANs and destination ports are in the same switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis. For example, in Figure 28-1, all traffic on port 5 (the source port) is mirrored to port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port 5.

Remote SPAN

RSPAN supports source ports, source VLANs, and destination ports on different switches, enabling remote monitoring of multiple switches across your network. Figure 28-2 shows source ports on Switch A and Switch B. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port, as shown on Switch C in the figure.
SPAN and RSPAN Concepts and Terminology

This section describes concepts and terminology associated with SPAN and RSPAN configuration.

SPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a destination port with source ports or source VLANs, all on a single network device. Local SPAN does not have separate source and destination sessions. Local SPAN sessions gather a set of ingress and egress packets specified by the user and form them into a stream of SPAN data, which is directed to the destination port.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN. The output of this session is the stream of SPAN packets that are sent to the RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.
An RSPAN source session is very similar to a local SPAN session, except for where the packet stream is directed. In an RSPAN source session, SPAN packets are relabeled with the RSPAN VLAN ID and directed over normal trunk ports to the destination switch.

An RSPAN destination session takes all packets received on the RSPAN VLAN, strips off the VLAN tagging, and presents them on the destination port. Its purpose is to present a copy of all RSPAN VLAN packets (except Layer 2 control packets) to the user for analysis.

There can be more than one source session and more than one destination session active in the same RSPAN VLAN. There can also be intermediate switches separating the RSPAN source and destination sessions. These switches need not be capable of running RSPAN, but they must respond to the requirements of the RSPAN VLAN (see the “RSPAN VLAN” section on page 28-8).

Traffic monitoring in a SPAN session has these restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- The switch supports up to two source sessions (local SPAN and RSPAN source sessions). You can run both a local SPAN and an RSPAN source session in the same switch. The switch supports a total of 66 source and RSPAN destination sessions.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- 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 RSPAN is enabled, each packet being monitored is transmitted twice, once as normal traffic and once as a monitored packet. Therefore monitoring a large number of ports or VLANs 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 or VLAN for that session.
- The switch does not support a combination of local SPAN and RSPAN in a single session. That is, an RSPAN source session cannot have a local destination port, an RSPAN destination session cannot have a local source port, and an RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same switch.

**Monitored Traffic**

SPAN sessions can monitor these traffic types:

- **Receive (Rx) SPAN**—The goal of receive (or ingress) SPAN is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that SPAN session.

  Packets that are modified because of routing or quality of service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.

  Features that can cause a packet to be dropped during receive processing have no effect on ingress SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These features include IP standard and extended input access control lists (ACLs), ingress QoS policing, VLAN ACLs, and egress QoS policing.
Understanding SPAN and RSPAN

Transmit (Tx) SPAN—The goal of transmit (or egress) SPAN is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that SPAN session. The copy is provided after the packet is modified.

Packets that are modified because of routing—for example, with modified time-to-live (TTL), MAC-address, or QoS values—are duplicated (with the modifications) at the destination port.

Features that can cause a packet to be dropped during transmit processing also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs and egress QoS policing.

Both—In a SPAN session, you can also monitor a port or VLAN for both received and sent packets. This is the default.

The default configuration for local SPAN session ports is to send all packets untagged. SPAN also does not normally monitor bridge protocol data unit (BPDU) packets and Layer 2 protocols, such as Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP), Spanning Tree Protocol (STP), and Port Aggregation Protocol (PAgP). However, when you enter the encapsulation replicate keywords when configuring a destination port, these changes occur:

- Packets are sent on the destination port with the same encapsulation—untagged, Inter-Switch Link (ISL), or IEEE 802.1Q—that they had on the source port.
- Packets of all types, including BPDU and Layer 2 protocol packets, are monitored.

Therefore, a local SPAN session with encapsulation replicate enabled can have a mixture of untagged, ISL, and IEEE 802.1Q tagged packets appear on the destination port.

Switch congestion can cause packets to be dropped at ingress source ports, egress source ports, or SPAN destination ports. In general, these characteristics are independent of one another. For example:

- A packet might be forwarded normally but dropped from monitoring due to an oversubscribed SPAN destination port.
- An ingress packet might be dropped from normal forwarding, but still appear on the SPAN destination port.
- An egress packet dropped because of switch congestion is also dropped from egress SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the Rx monitor on port A and Tx monitor on port B. If a packet enters the switch through port A and is switched to port B, both incoming and outgoing packets are sent to the destination port. Both packets are the same (unless a Layer-3 rewrite occurs, in which case the packets are different because of the packet modification).

Source Ports

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis. In a local SPAN session or RSPAN source session, you can monitor source ports or VLANs for traffic in one or both directions. The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs (up to the maximum number of VLANs supported). However, the switch supports a maximum of two sessions (local or RSPAN) with source ports or VLANs, and you cannot mix ports and VLANs in a single session.
A source port has these characteristics:

- It can be monitored in multiple SPAN sessions.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor.
- It can be any port type (for example, EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth).
- For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a physical port as it participates in the port channel.
- It can be an access port, trunk port, routed port, or voice VLAN port.
- It cannot be a destination port.
- Source ports can be in the same or different VLANs.
- You can monitor multiple source ports in a single session.

Source VLANs

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs. The SPAN or RSPAN source interface in VSPAN is a VLAN ID, and traffic is monitored on all the ports for that VLAN.

VSPAN has these characteristics:

- All active ports in the source VLAN are included as source ports and can be monitored in either or both directions.
- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources being monitored.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

VLAN Filtering

When you monitor a trunk port as a source port, by default, all VLANs active on the trunk are monitored. You can limit SPAN traffic monitoring on trunk source ports to specific VLANs by using VLAN filtering.

- VLAN filtering applies only to trunk ports or to voice VLAN ports.
- VLAN filtering applies only to port-based sessions and is not allowed in sessions with VLAN sources.
- When a VLAN filter list is specified, only those VLANs in the list are monitored on trunk ports or on voice VLAN access ports.
- SPAN traffic coming from other port types is not affected by VLAN filtering; that is, all VLANs are allowed on other ports.
- VLAN filtering affects only traffic forwarded to the destination SPAN port and does not affect the switching of normal traffic.
Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer.

A destination port has these characteristics:

- For a local SPAN session, the destination port must reside on the same switch as the source port. For an RSPAN session, it is located on the switch containing the RSPAN destination session. There is no destination port on a switch running only an RSPAN source session.
- When a port is configured as a SPAN destination port, the configuration overwrites the original port configuration. When the SPAN destination configuration is removed, the port reverts to its previous configuration. If a configuration change is made to the port while it is acting as a SPAN destination port, the change does not take effect until the SPAN destination configuration had been removed.
- If the port was in an EtherChannel group, it is removed from the group while it is a destination port. If it was a routed port, it is no longer a routed port.
- It can be any Ethernet physical port.
- It cannot be a secure port.
- It cannot be a source port.
- It cannot be an EtherChannel group or a VLAN.
- It can participate in only one SPAN session at a time (a destination port in one SPAN session cannot be a destination port for a second SPAN session).
- When it is active, incoming traffic is disabled. The port does not transmit any traffic except that required for the SPAN session. Incoming traffic is never learned or forwarded on a destination port.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- It does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- The maximum number of destination ports in a switch is 64.

Local SPAN and RSPAN destination ports behave differently regarding VLAN tagging and encapsulation:

- For local SPAN, if the encapsulation replicate keywords are specified for the destination port, these packets appear with the original encapsulation (untagged, ISL, or IEEE 802.1Q). If these keywords are not specified, packets appear in the untagged format. Therefore, the output of a local SPAN session with encapsulation replicate enabled can contain a mixture of untagged, ISL, or IEEE 802.1Q-tagged packets.
- For RSPAN, the original VLAN ID is lost because it is overwritten by the RSPAN VLAN identification. Therefore, all packets appear on the destination port as untagged.
RSPAN VLAN

The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. It has these special characteristics:

- All traffic in the RSPAN VLAN is always flooded.
- No MAC address learning occurs on the RSPAN VLAN.
- RSPAN VLAN traffic only flows on trunk ports.
- RSPAN VLANs must be configured in VLAN configuration mode by using the `remote-span` VLAN configuration mode command.
- STP can run on RSPAN VLAN trunks but not on SPAN destination ports.
- An RSPAN VLAN cannot be a private-VLAN primary or secondary VLAN.

For VLANs 1 to 1005 that are visible to VLAN Trunking Protocol (VTP), the VLAN ID and its associated RSPAN characteristic are propagated by VTP. If you assign an RSPAN VLAN ID in the extended VLAN range (1006 to 4094), you must manually configure all intermediate switches.

It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

SPAN and RSPAN Interaction with Other Features

SPAN interacts with these features:

- Routing—SPAN does not monitor routed traffic. VSPAN only monitors traffic that enters or exits the switch, not traffic that is routed between VLANs. For example, if a VLAN is being Rx-monitored and the switch routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and not received on the SPAN destination port.
- STP—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.
- CDP—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP.
- VTP—You can use VTP to prune an RSPAN VLAN between switches.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source or destination ports at any time. However, changes in VLAN membership or trunk settings for a destination port do not take effect until you remove the SPAN destination configuration. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the respective SPAN sessions automatically adjust accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port but not as a SPAN destination port. When a group is configured as a SPAN source, the entire group is monitored.

If a physical port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list.
A physical port that belongs to an EtherChannel group can be configured as a SPAN source port and still be a part of the EtherChannel. In this case, data from the physical port is monitored as it participates in the EtherChannel. However, if a physical port that belongs to an EtherChannel group is configured as a SPAN destination, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the *inactive* or *suspended* state.

If a physical port that belongs to an EtherChannel group is a destination port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.

- Multicast traffic can be monitored. For egress and ingress port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times the multicast packet is sent.
- A private-VLAN port cannot be a SPAN destination port.
- A secure port cannot be a SPAN destination port.

For SPAN sessions, do not enable port security on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable port security on any ports with monitored egress.

- An IEEE 802.1x port can be a SPAN source port. You can enable IEEE 802.1x on a port that is a SPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination.

For SPAN sessions, do not enable IEEE 802.1x on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable IEEE 802.1x on any ports that are egress monitored.

## Configuring SPAN and RSPAN

These sections contain this configuration information:

- Default SPAN and RSPAN Configuration, page 28-10
- Configuring Local SPAN, page 28-10
- Configuring RSPAN, page 28-16
Default SPAN and RSPAN Configuration

Table 28-1 shows the default SPAN and RSPAN configuration.

Table 28-1  Default SPAN and RSPAN Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPAN state (SPAN and RSPAN)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Source port traffic to monitor</td>
<td>Both received and sent traffic (both).</td>
</tr>
<tr>
<td>Encapsulation type (destination port)</td>
<td>Native form (untagged packets).</td>
</tr>
<tr>
<td>Ingress forwarding (destination port)</td>
<td>Disabled.</td>
</tr>
<tr>
<td>VLAN filtering</td>
<td>On a trunk interface used as a source port, all VLANs are monitored.</td>
</tr>
<tr>
<td>RSPAN VLANs</td>
<td>None configured.</td>
</tr>
</tbody>
</table>

Configuring Local SPAN

These sections contain this configuration information:
- SPAN Configuration Guidelines, page 28-10
- Creating a Local SPAN Session, page 28-11
- Creating a Local SPAN Session and Configuring Incoming Traffic, page 28-14
- Specifying VLANs to Filter, page 28-15

SPAN Configuration Guidelines

Follow these guidelines when configuring SPAN:
- For SPAN sources, you can monitor traffic for a single port or VLAN or a series or range of ports or VLANs for each session. You cannot mix source ports and source VLANs within a single SPAN session.
- The destination port cannot be a source port; a source port cannot be a destination port.
- You cannot have two SPAN sessions using the same destination port.
- When you configure a switch port as a SPAN destination port, it is no longer a normal switch port; only monitored traffic passes through the SPAN destination port.
- Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the `no monitor session {session_number | all | local | remote}` global configuration command to delete configured SPAN parameters.
- For local SPAN, outgoing packets through the SPAN destination port carry the original encapsulation headers—untagged, ISL, or IEEE 802.1Q—if the `encapsulation replicate` keywords are specified. If the keywords are not specified, the packets are sent in native form. For RSPAN destination ports, outgoing packets are not tagged.
- 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 or source VLAN are enabled.
You can limit SPAN traffic to specific VLANs by using the `filter vlan` keyword. If a trunk port is being monitored, only traffic on the VLANs specified with this keyword is monitored. By default, all VLANs are monitored on a trunk port.

You cannot mix source VLANs and filter VLANs within a single SPAN session.

Catalyst 3560-24PS and 3560-48PS switches have hardware limitations related to SPAN. An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the `replicate` option.

On Catalyst 3560-24PS and 3560-48PS switches, egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the encapsulation replicate option is used. This limitation does not apply to bridged packets. The workaround is to use the `encapsulate replicate` keywords in the `monitor session` global configuration command.

### Creating a Local SPAN Session

Beginning in privileged EXEC mode, follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| Step 2  | no monitor session 
(session_number | all | local | remote) | Remove any existing SPAN configuration for the session. For `session_number`, the range is 1 to 66. Specify `all` to remove all SPAN sessions, `local` to remove all local sessions, or `remote` to remove all remote SPAN sessions. |
### Step 3

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `monitor session session_number source {interface interface-id | vlan vlan-id} [ | - ] [both | rx | tx]` | Specify the SPAN session and the source port (monitored port).
| | For `session_number`, the range is 1 to 66.
| | For `interface-id`, specify the source port or source VLAN to monitor.
| | - For source `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 48.
| | - For `vlan-id`, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).
| | **Note** A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session.
| | (Optional) `[ | - ]` Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.
| | (Optional) Specify the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic.
| | - `both`—Monitor both received and sent traffic. This is the default.
| | - `rx`—Monitor received traffic.
| | - `tx`—Monitor sent traffic.
| | **Note** You can use the `monitor session session_number source` command multiple times to configure multiple source ports.

### Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `monitor session session_number destination {interface interface-id [ | - ] [encapsulation replicate]}` | Specify the SPAN session and the destination port (monitoring port).
| | For `session_number`, specify the session number entered in step 3.
| | **Note** For local SPAN, you must use the same session number for the source and destination interfaces.
| | For `interface-id`, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.
| | (Optional) `[ | - ]` Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.
| | (Optional) Enter `encapsulation replicate` to specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).
| | **Note** You can use `monitor session session_number destination` command multiple times to configure multiple destination ports.

### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To delete a SPAN session, use the `no monitor session session_number` global configuration command. To remove a source or destination port or VLAN from the SPAN session, use the `no monitor session session_number source {interface interface-id | vlan vlan-id}` global configuration command or the `no monitor session session_number destination interface interface-id` global configuration command. For destination interfaces, the encapsulation options are ignored with the `no` form of the command.

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(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(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(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(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```
Chapter 28      Configuring SPAN and RSPAN

Creating a Local SPAN Session and Configuring Incoming Traffic

Beginning in privileged EXEC mode, 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).

For details about the keywords not related to incoming traffic, see the “Creating a Local SPAN Session” section on page 28-11.

<table>
<thead>
<tr>
<th>Command</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> no monitor session {session_number</td>
<td>all</td>
</tr>
<tr>
<td><strong>Step 3</strong> monitor session session_number source {interface interface-id</td>
<td>vlan vlan-id} [both</td>
</tr>
<tr>
<td><strong>Step 4</strong> monitor session session_number destination {interface interface-id [,</td>
<td>-] [encapsulation replicate] [ingress {dot1q vlan vlan-id</td>
</tr>
<tr>
<td>For session_number, specify the session number entered in Step 3.</td>
<td>For interface-id, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.</td>
</tr>
<tr>
<td>(Optional) [,</td>
<td>-] Specify a series or range of interfaces. Enter a space before and after the comma or hyphen.</td>
</tr>
<tr>
<td>Enter ingress with keywords to enable forwarding of incoming traffic on the destination port and to specify the encapsulation type:</td>
<td>Enter ingress with keywords to enable forwarding of incoming traffic on the destination port and to specify the encapsulation type:</td>
</tr>
<tr>
<td>• dot1q vlan vlan-id—Accept incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.</td>
<td>• dot1q vlan vlan-id—Accept incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.</td>
</tr>
<tr>
<td>• isl—Forward ingress packets with ISL encapsulation.</td>
<td>• isl—Forward ingress packets with ISL encapsulation.</td>
</tr>
<tr>
<td>• untagged vlan vlan-id or vlan vlan-id—Accept incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.</td>
<td>• untagged vlan vlan-id or vlan vlan-id—Accept incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show monitor [session session_number] show running-config</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Save the configuration in the configuration file.</td>
</tr>
</tbody>
</table>

To delete a SPAN session, use the no monitor session session_number global configuration command.

To remove a source or destination port or VLAN from the SPAN session, use the no monitor session session_number source {interface interface-id | vlan vlan-id} global configuration command or the no
**monitor session** `session_number destination interface interface-id` global configuration command. For destination interfaces, the encapsulation and ingress options are ignored with the `no` form of the command.

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 IEEE 802.1Q encapsulation and VLAN 6 as the default ingress VLAN.

```plaintext
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 dot1q vlan 6
Switch(config)# end
```

**Specifying VLANs to Filter**

Beginning in privileged EXEC mode, follow these steps to limit SPAN source traffic to specific VLANs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **2** | no monitor session `{session_number | all | local | remote}` | Remove any existing SPAN configuration for the session.  
For `session_number`, the range is 1 to 66.  
Specify `all` to remove all SPAN sessions, `local` to remove all local sessions, or `remote` to remove all remote SPAN sessions. |
| **3** | monitor session `session_number source interface interface-id` | Specify the characteristics of the source port (monitored port) and SPAN session.  
For `session_number`, the range is 1 to 66.  
For `interface-id`, specify the source port to monitor. The interface specified must already be configured as a trunk port. |
| **4** | monitor session `session_number filter vlan vlan-id [, ]-` | Limit the SPAN source traffic to specific VLANs.  
For `session_number`, enter the session number specified in Step 3.  
For `vlan-id`, the range is 1 to 4094.  
(Optional) Use a comma (,) to specify a series of VLANs, or use a hyphen (-) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen. |
| **5** | monitor session `session_number destination {interface interface-id [, ]-} [encapsulation replicate]` | Specify the SPAN session and the destination port (monitoring port).  
For `session_number`, specify the session number entered in Step 3.  
For `interface-id`, specify the destination port. The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.  
(Optional) [, ]- Specify a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.  
(Optional) Enter `encapsulation replicate` to specify that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). |
### Configuring SPAN and RSPAN

**Chapter 28**  
**Configuring SPAN and RSPAN**

#### Configuring SPAN and RSPAN

To monitor all VLANs on the trunk port, use the `no monitor session session_number filter` global configuration command.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and VLAN 9 to destination Gigabit Ethernet port 1.

```plaintext
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet0/1
Switch(config)# end
```

### Configuring RSPAN

These sections contain this configuration information:

- RSPAN Configuration Guidelines, page 28-16
- Configuring a VLAN as an RSPAN VLAN, page 28-17
- Creating an RSPAN Source Session, page 28-18
- Creating an RSPAN Destination Session, page 28-20
- Creating an RSPAN Destination Session and Configuring Incoming Traffic, page 28-21
- Specifying VLANs to Filter, page 28-22

### RSPAN Configuration Guidelines

Follow these guidelines when configuring RSPAN:

- All the items in the “SPAN Configuration Guidelines” section on page 28-10 apply to RSPAN.
- As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.
- You can apply an output ACL to RSPAN traffic to selectively filter or monitor specific packets. Specify these ACLs on the RSPAN VLAN in the RSPAN source switches.
- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple switches in your network.
- RSPAN does not support BPDU packet monitoring or other Layer 2 switch protocols.
- The RSPAN VLAN is configured only on trunk ports and not on access ports. To avoid unwanted traffic in RSPAN VLANs, make sure that the VLAN remote-span feature is supported in all the participating switches.
- Access ports (including voice VLAN ports) on the RSPAN VLAN are put in the inactive state.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show monitor [session session_number]</code> Verify the configuration.</td>
</tr>
<tr>
<td></td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>copy running-config startup-config</code> (Optional) Save the configuration in the configuration file.</td>
</tr>
</tbody>
</table>

---

To monitor all VLANs on the trunk port, use the `no monitor session session_number filter` global configuration command.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and VLAN 9 to destination Gigabit Ethernet port 1.

```plaintext
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5, 9
Switch(config)# monitor session 2 destination interface gigabitethernet0/1
Switch(config)# end
```
Chapter 28  Configuring SPAN and RSPAN

- RSPAN VLANs are included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. RSPAN VLANs can also be sources in SPAN sessions. However, since the switch does not monitor spanned traffic, it does not support egress spanning of packets on any RSPAN VLAN identified as the destination of an RSPAN source session on the switch.

- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The same RSPAN VLAN is used for an RSPAN session in all the switches.
  - All participating switches support RSPAN.

- We recommend that you configure an RSPAN VLAN before you configure an RSPAN source or a destination session.

- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN IDs that are lower than 1005.

- Catalyst 3560-24PS and 3560-48PS switches have hardware limitations related to RSPAN:
  - An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the replicate option. For a remote SPAN session, there is no workaround.
  - Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. There is no workaround.
  - During periods of very high traffic, when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session.

Configuring a VLAN as an RSPAN VLAN

First create a new VLAN to be the RSPAN VLAN for the RSPAN session. You must create the RSPAN VLAN in all switches that will participate in RSPAN. If the RSPAN VLAN-ID is in the normal range (lower than 1005) and VTP is enabled in the network, you can create the RSPAN VLAN in one switch, and VTP propagates it to the other switches in the VTP domain. For extended-range VLANs (greater than 1005), you must configure RSPAN VLAN on both source and destination switches and any intermediate switches.

Use VTP pruning to get an efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

Beginning in privileged EXEC mode, follow these steps to create an RSPAN VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>vlan vlan-id</td>
<td>Enter a VLAN ID to create a VLAN, or enter the VLAN ID of an existing VLAN, and enter VLAN configuration mode. The range is 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 through 1005 (reserved for Token Ring and FDDI VLANs).</td>
</tr>
</tbody>
</table>
Configuring SPAN and RSPAN

Chapter 28 Configuring SPAN and RSPAN

Configuring SPAN and RSPAN

To remove the remote SPAN characteristic from a VLAN and convert it back to a normal VLAN, use the `no remote-span` VLAN configuration command.

This example shows how to create RSPAN VLAN 901.

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

Creating an RSPAN Source Session

Beginning in privileged EXEC mode, follow these steps to start an RSPAN source session and to specify the monitored source and the destination RSPAN VLAN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>remote-span</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the remote SPAN characteristic from a VLAN and convert it back to a normal VLAN, use the `no remote-span` VLAN configuration command.

This example shows how to create RSPAN VLAN 901.

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no monitor session `[session_number</td>
</tr>
</tbody>
</table>
To delete a SPAN session, use the no monitor session session_number global configuration command.

To remove a source port or VLAN from the SPAN session, use the no monitor session session_number source {interface interface-id | vlan vlan-id} global configuration command. To remove the RSPAN VLAN from the session, use the no monitor session session_number destination remote vlan vlan-id.

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901.

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet0/2 rx

Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```
Creating an RSPAN Destination Session

You configure the RSPAN destination session on a different switch; that is, not the switch on which the source session was configured.

Beginning in privileged EXEC mode, follow these steps to define the RSPAN VLAN on that switch, to create an RSPAN destination session, and to specify the source RSPAN VLAN and the destination port:

<table>
<thead>
<tr>
<th>Command</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> vlan vlan-id</td>
<td>Enter the VLAN ID of the RSPAN VLAN created from the source switch, and enter VLAN configuration mode. If both switches are participating in VTP and the RSPAN VLAN ID is from 2 to 1005, Steps 2 through 4 are not required because the RSPAN VLAN ID is propagated through the VTP network.</td>
</tr>
<tr>
<td><strong>Step 3</strong> remote-span</td>
<td>Identify the VLAN as the RSPAN VLAN.</td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> no monitor session {session_number</td>
<td>all</td>
</tr>
<tr>
<td><strong>Step 6</strong> monitor session session_number source remote vlan vlan-id</td>
<td>Specify the RSPAN session and the source RSPAN VLAN. For session_number, the range is 1 to 66. For vlan-id, specify the source RSPAN VLAN to monitor.</td>
</tr>
<tr>
<td><strong>Step 7</strong> monitor session session_number destination interface interface-id</td>
<td>Specify the RSPAN session and the destination interface. For session_number, enter the number defined in Step 6. In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port. For interface-id, specify the destination interface. The destination interface must be a physical interface. Though visible in the command-line help string, encapsulation replicate is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged.</td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong> show monitor [session session_number] show running-config</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 10</strong> copy running-config startup-config</td>
<td>(Optional) Save the configuration in the configuration file.</td>
</tr>
</tbody>
</table>

To delete a SPAN session, use the no monitor session session_number global configuration command. To remove a destination port from the SPAN session, use the no monitor session session_number destination interface interface-id global configuration command. To remove the RSPAN VLAN from the session, use the no monitor session session_number source remote vlan vlan-id.
This example shows how to configure VLAN 901 as the source remote VLAN and port 1 as the destination interface:

```plaintext
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet0/1
Switch(config)# end
```

### Creating an RSPAN Destination Session and Configuring Incoming Traffic

Beginning in privileged EXEC mode, follow these steps to create an RSPAN destination session, to specify the source RSPAN VLAN and the destination port, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

For details about the keywords not related to incoming traffic, see the “Creating an RSPAN Destination Session” section on page 28-20. This procedure assumes that the RSPAN VLAN has already been configured.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no monitor session {session_number</td>
</tr>
<tr>
<td>Step 3</td>
<td>monitor session session_number source remote vlan vlan-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>monitor session session_number destination {interface interface-id</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
</tbody>
</table>
Chapter 28  Configuring SPAN and RSPAN

Configuring SPAN and RSPAN

To delete an RSPAN session, use the `no monitor session session_number` global configuration command. To remove a destination port from the RSPAN session, use the `no monitor session session_number destination interface interface-id` global configuration command. The ingress options are ignored with the `no` form of the command.

This example shows how to configure VLAN 901 as the source remote VLAN in RSPAN session 2, to configure Gigabit Ethernet source port 2 as the destination interface, and to enable forwarding of incoming traffic on the interface with VLAN 6 as the default receiving VLAN.

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress vlan 6
Switch(config)# end
```

### Specifying VLANs to Filter

Beginning in privileged EXEC mode, follow these steps to configure the RSPAN source session to limit RSPAN source traffic to specific VLANs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no monitor session `{ session_number</td>
</tr>
<tr>
<td>Step 3</td>
<td>monitor session <code>session_number source interface interface-id</code></td>
</tr>
<tr>
<td>Step 4</td>
<td>monitor session <code>session_number filter vlan vlan-id [ , 1 - ]</code></td>
</tr>
</tbody>
</table>
## Chapter 28  Configuring SPAN and RSPAN

**Displaying SPAN and RSPAN Status**

To display the current SPAN or RSPAN configuration, use the `show monitor` user EXEC command. You can also use the `show running-config` privileged EXEC command to display configured SPAN or RSPAN sessions.

### Command Purpose

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session <code>session_number</code> destination remote vlan <code>vlan-id</code></td>
<td>Specify the RSPAN session and the destination remote VLAN (RSPAN VLAN). For <code>session_number</code>, enter the session number specified in step 3. For <code>vlan-id</code>, specify the RSPAN VLAN to carry the monitored traffic to the destination port.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show monitor [session <code>session_number</code>]</td>
<td>Verify the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save the configuration in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

To monitor all VLANs on the trunk port, use the `no monitor session `session_number` filter vlan` global configuration command.

This example shows how to remove any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on trunk port 2, and send traffic for only VLANs 1 through 5 and 9 to destination RSPAN VLAN 902.

Switch(config)# no monitor session 2  
Switch(config)# monitor session 2 source interface gigabitethernet0/2 rx  
Switch(config)# monitor session 2 filter vlan 1 - 5, 9  
Switch(config)# monitor session 2 destination remote vlan 902  
Switch(config)# end
Configuring RMON

This chapter describes how to configure Remote Network Monitoring (RMON) on the Catalyst 3560 switch.

RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.

Note

For complete syntax and usage information for the commands used in this chapter, see the “System Management Commands” section in the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Understanding RMON, page 29-2
- Configuring RMON, page 29-3
- Displaying RMON Status, page 29-7
Understanding RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments as shown in Figure 29-1.

Figure 29-1  Remote Monitoring Example

The switch supports these RMON groups (defined in RFC 1757):

- **Statistics (RMON group 1)**—Collects Ethernet statistics (including Fast Ethernet and Gigabit Ethernet statistics, depending on the switch type and supported interfaces) on an interface.
- **History (RMON group 2)**—Collects a history group of statistics on Ethernet ports (including Fast Ethernet and Gigabit Ethernet statistics, depending on the switch type and supported interfaces) for a specified polling interval.
- **Alarm (RMON group 3)**—Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- **Event (RMON group 9)**—Specifies the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

Because switches supported by this software release use hardware counters for RMON data processing, the monitoring is more efficient, and little processing power is required.

- **Note**: 64-bit counters are not supported for RMON alarms.
Configuring RMON

These sections contain this configuration information:

- Default RMON Configuration, page 29-3
- Configuring RMON Alarms and Events, page 29-3 (required)
- Collecting Group History Statistics on an Interface, page 29-5 (optional)
- Collecting Group Ethernet Statistics on an Interface, page 29-6 (optional)

Default RMON Configuration

RMON is disabled by default; no alarms or events are configured.

Configuring RMON Alarms and Events

You can configure your switch for RMON by using the command-line interface (CLI) or an SNMP-compatible network management station. We recommend that you use a generic RMON console application on the network management station (NMS) to take advantage of the RMON network management capabilities. You must also configure SNMP on the switch to access RMON MIB objects. For more information, see Chapter 31, “Configuring SNMP.”

Note

64-bit counters are not supported for RMON alarms.
Beginning in privileged EXEC mode, follow these steps to enable RMON alarms and events. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>rmon alarm number variable interval {absolute</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></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>rmon event number [description string] [log] [owner string] [trap community]</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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
To disable an alarm, use the `no rmon alarm number` global configuration command on each alarm you configured. You cannot disable at once all the alarms that you configured. To disable an event, use the `no rmon event number` global configuration command. To learn more about alarms and events and how they interact with each other, see RFC 1757.

You can set an alarm on any MIB object. The following example configures RMON alarm number 10 by using the `rmon alarm` command. The alarm monitors the MIB variable `ifEntry.20.1` once every 20 seconds until the alarm is disabled and checks the change in the variable’s rise or fall. If the `ifEntry.20.1` value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the `rmon event` command. Possible events can include a log entry or an SNMP trap. If the `ifEntry.20.1` value changes by 0, the alarm is reset and can be triggered again.

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner jjohnson
```

The following example creates RMON event number 1 by using the `rmon event` command. The event is defined as `High ifOutErrors` and generates a log entry when the event is triggered by the alarm. The user `jjones` owns the row that is created in the event table by this command. This example also generates an SNMP trap when the event is triggered.

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner jjones
```

## Collecting Group History Statistics on an Interface

You must first configure RMON alarms and events to display collection information.

Beginning in privileged EXEC mode, follow these steps to collect group history statistics on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface on which to collect history, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 rmon collection history index [buckets bucket-number] [interval seconds] [owner ownername]</td>
<td>Enable history collection for the specified number of buckets and time period.</td>
</tr>
<tr>
<td></td>
<td>- For <code>index</code>, identify the RMON group of statistics The range is 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <code>buckets bucket-number</code>, specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1 to 65535. The default is 50 buckets.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <code>interval seconds</code>, specify the number of seconds in each polling cycle. The range is 1 to 3600. The default is 1800 seconds.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) For <code>owner ownername</code>, enter the name of the owner of the RMON group of statistics.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>
To disable history collection, use the `no rmon collection history index` interface configuration command.

### Collecting Group Ethernet Statistics on an Interface

Beginning in privileged EXEC mode, follow these steps to collect group Ethernet statistics on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: interface interface-id</td>
<td>Specify the interface on which to collect statistics, and enter</td>
</tr>
<tr>
<td></td>
<td>interface configuration mode.</td>
</tr>
<tr>
<td>Step 3: rmon collection stats index</td>
<td>Enable RMON statistic collection on the interface.</td>
</tr>
<tr>
<td></td>
<td>• For <code>index</code>, specify the RMON group of statistics. The range</td>
</tr>
<tr>
<td></td>
<td>is from 1 to 65535.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>owner ownername</code>, enter the name of the owner of the</td>
</tr>
<tr>
<td></td>
<td>RMON group of statistics.</td>
</tr>
<tr>
<td>Step 4: end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5: show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6: show rmon statistics</td>
<td>Display the contents of the switch statistics table.</td>
</tr>
<tr>
<td>Step 7: copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the collection of group Ethernet statistics, use the `no rmon collection stats index` interface configuration command.

This example shows how to collect RMON statistics for the owner `root`:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```
Displaying RMON Status

To display the RMON status, use one or more of the privileged EXEC commands in Table 29-1:

Table 29-1  Commands for Displaying RMON Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show rmon</td>
<td>Displays general RMON statistics.</td>
</tr>
<tr>
<td>show rmon alarms</td>
<td>Displays the RMON alarm table.</td>
</tr>
<tr>
<td>show rmon events</td>
<td>Displays the RMON event table.</td>
</tr>
<tr>
<td>show rmon history</td>
<td>Displays the RMON history table.</td>
</tr>
<tr>
<td>show rmon statistics</td>
<td>Displays the RMON statistics table.</td>
</tr>
</tbody>
</table>

For information about the fields in these displays, see the “System Management Commands” section in the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.
Displaying RMON Status
Configuring System Message Logging

This chapter describes how to configure system message logging on the Catalyst 3560 switch.

**Note**
For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* from the Cisco.com page under **Documentation > Cisco IOS Software > 12.2 Mainline > Command References**.

This chapter consists of these sections:
- Understanding System Message Logging, page 30-1
- Configuring System Message Logging, page 30-2
- Displaying the Logging Configuration, page 30-13

**Caution**
Logging messages to the console at a high rate can cause high CPU utilization and adversely affect how the switch operates.

Understanding 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.

**Note**
The syslog format is compatible with 4.3 BSD UNIX.

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 console 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.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet or through the console port.

Configuring System Message Logging

These sections contain this configuration information:

- System Log Message Format, page 30-2
- Default System Message Logging Configuration, page 30-3
- Disabling Message Logging, page 30-4 (optional)
- Setting the Message Display Destination Device, page 30-5 (optional)
- Synchronizing Log Messages, page 30-6 (optional)
- Enabling and Disabling Time Stamps on Log Messages, page 30-7 (optional)
- Enabling and Disabling Sequence Numbers in Log Messages, page 30-8 (optional)
- Defining the Message Severity Level, page 30-8 (optional)
- Limiting Syslog Messages Sent to the History Table and to SNMP, page 30-10 (optional)
- Enabling the Configuration-Change Logger, page 30-10 (optional)
- Configuring UNIX Syslog Servers, page 30-11 (optional)

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. Messages appear in this format:

```
seq no:timestamp: %facility-severity-MNEMONIC:description
```

The part of the message preceding the percent sign depends on the setting of the service sequence-numbers, service timestamps log datetime, service timestamps log datetime [localtime] [msec] [show-timezone], or service timestamps log uptime global configuration command.
Table 30-1 describes the elements of syslog messages.

### Table 30-1  System Log Message Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seq no:</td>
<td>Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. For more information, see the “Enabling and Disabling Sequence Numbers in Log Messages” section on page 30-8.</td>
</tr>
<tr>
<td>timestamp formats:</td>
<td></td>
</tr>
<tr>
<td>mm/dd hh:mm:ss or hh:mm:ss (short uptime) or d h (long uptime)</td>
<td>Date and time of the message or event. This information appears only if the service timestamps log [datetime</td>
</tr>
<tr>
<td>facility</td>
<td>The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 30-4 on page 30-13.</td>
</tr>
<tr>
<td>severity</td>
<td>Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 30-3 on page 30-9.</td>
</tr>
<tr>
<td>MNEMONIC</td>
<td>Text string that uniquely describes the message.</td>
</tr>
<tr>
<td>description</td>
<td>Text string containing detailed information about the event being reported.</td>
</tr>
</tbody>
</table>

This example shows a partial switch system message:

```
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 2
*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)
```

### Default System Message Logging Configuration

Table 30-2 shows the default system message logging configuration.

#### Table 30-2  Default System Message Logging Configuration

<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 (and numerically lower levels; see Table 30-3 on page 30-9).</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>
</tbody>
</table>

Catalyst 3560 Switch Software Configuration Guide
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.

Beginning in privileged EXEC mode, follow these steps to disable message logging. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>no logging console</td>
<td>Disable message logging.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>or show logging</td>
<td></td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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. For more information, see the “Synchronizing Log Messages” section on page 30-6.

To re-enable message logging after it has been disabled, use the `logging on` global configuration command.
Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>logging buffered [size]</code></td>
</tr>
<tr>
<td></td>
<td>Note</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>logging host</code></td>
</tr>
<tr>
<td></td>
<td>For <code>host</code>, specify the name or IP address of the host to be used as the syslog server.</td>
</tr>
<tr>
<td></td>
<td>To build a list of syslog servers that receive logging messages, enter this command more than once.</td>
</tr>
<tr>
<td></td>
<td>For complete syslog server configuration steps, see the “Configuring UNIX Syslog Servers” section on page 30-11.</td>
</tr>
<tr>
<td></td>
<td>• For <code>filename</code>, enter the log message filename.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>max-file-size</code>, specify the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>min-file-size</code>, specify the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For `severity-level-number</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>terminal monitor</code></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>
The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the **clear logging** privileged EXEC command.

Use the **logging event power-inline-status** interface configuration command to enable and to disable logging of Power over Ethernet (PoE) events on specific PoE-capable ports. Logging on these ports is enabled by default.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a file, use the **no logging file** [severity-level-number | type] global configuration command.

### 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.

Beginning in privileged EXEC mode, follow these steps to configure synchronous logging. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Specify the line to be configured for synchronous logging of messages.</td>
</tr>
<tr>
<td><strong>line [console \ vty] line-number</strong></td>
<td>• Use the <strong>console</strong> keyword for configurations that occur through the switch console port.</td>
</tr>
<tr>
<td><strong>[ending-line-number]</strong></td>
<td>• Use the <strong>line vty line-number</strong> command to specify 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>You can change the setting of all 16 vty lines at once by entering:</td>
<td>You can change the setting of all 16 vty lines at once by entering:</td>
</tr>
<tr>
<td><strong>line vty 0 15</strong></td>
<td><strong>line vty 0 15</strong></td>
</tr>
<tr>
<td>Or you can 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>
<td>Or you can 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><strong>line vty 2</strong></td>
<td><strong>line vty 2</strong></td>
</tr>
<tr>
<td>When you enter this command, the mode changes to line configuration.</td>
<td>When you enter this command, the mode changes to line configuration.</td>
</tr>
</tbody>
</table>
Configuring System Message Logging

## Chapter 30

### Configuring System Message Logging

To disable synchronization of unsolicited messages and debug output, use the `no logging synchronous [level severity-level | all] [limit number-of-buffers]` line configuration command.

### Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time-stamped.

Beginning in privileged EXEC mode, follow these steps to enable time-stamping of log messages. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 service timestamps log uptime</td>
<td>Enable log time stamps.</td>
</tr>
<tr>
<td>or</td>
<td>The first command enables time stamps on log messages, showing the time since the system was rebooted.</td>
</tr>
<tr>
<td>service timestamps log datetime [msec] [localtime] [show-timezone]</td>
<td>The second command enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time-zone, and the time zone name.</td>
</tr>
</tbody>
</table>

To disable time stamps for both debug and log messages, use the `no service timestamps` global configuration command.

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)
```
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

### Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same time stamp, you can display messages with sequence numbers so that you can unambiguously see a single message. By default, sequence numbers in log messages are not displayed.

Beginning in privileged EXEC mode, follow these steps to enable sequence numbers in log messages. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>service sequence-numbers</code></td>
<td>Enable sequence numbers.</td>
</tr>
<tr>
<td>Step 3: <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4: <code>show running-config</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5: <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable sequence numbers, use the `no service sequence-numbers` global configuration command.

This example shows part of a logging display with sequence numbers enabled:

000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

### Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in Table 30-3.

Beginning in privileged EXEC mode, follow these steps to define the message severity level. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>logging console level</code></td>
<td>Limit messages logged to the console.</td>
</tr>
<tr>
<td></td>
<td>By default, the console receives debugging messages and numerically lower levels (see Table 30-3 on page 30-9).</td>
</tr>
<tr>
<td>Step 3: <code>logging monitor level</code></td>
<td>Limit messages logged to the terminal lines.</td>
</tr>
<tr>
<td></td>
<td>By default, the terminal receives debugging messages and numerically lower levels (see Table 30-3 on page 30-9).</td>
</tr>
</tbody>
</table>
Configuring System Message Logging

Note
Specifying a level causes messages at that level and numerically lower levels to appear at the destination.

To disable logging to the console, use the no logging console global configuration command. To disable logging to a terminal other than the console, use the no logging monitor global configuration command. To disable logging to syslog servers, use the no logging trap global configuration command.

Table 30-3 describes the level keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 30-3 Message Logging Level Keywords

<table>
<thead>
<tr>
<th>Level Keyword</th>
<th>Level</th>
<th>Description</th>
<th>Syslog Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergencies</td>
<td>0</td>
<td>System unstable</td>
<td>LOG_EMERG</td>
</tr>
<tr>
<td>alerts</td>
<td>1</td>
<td>Immediate action needed</td>
<td>LOG_ALERT</td>
</tr>
<tr>
<td>critical</td>
<td>2</td>
<td>Critical conditions</td>
<td>LOG_CRIT</td>
</tr>
<tr>
<td>errors</td>
<td>3</td>
<td>Error conditions</td>
<td>LOG_ERR</td>
</tr>
<tr>
<td>warnings</td>
<td>4</td>
<td>Warning conditions</td>
<td>LOG_WARNING</td>
</tr>
<tr>
<td>notifications</td>
<td>5</td>
<td>Normal but significant condition</td>
<td>LOG_NOTICE</td>
</tr>
<tr>
<td>informational</td>
<td>6</td>
<td>Informational messages only</td>
<td>LOG_INFO</td>
</tr>
<tr>
<td>debugging</td>
<td>7</td>
<td>Debugging messages</td>
<td>LOG_DEBUG</td>
</tr>
</tbody>
</table>

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels warnings through emergencies. These types of messages mean that the functionality of the switch is affected. For information on how to recover from these malfunctions, see the system message guide for this release.
- Output from the debug commands, displayed at the debugging level. Debug commands are typically used only by the Technical Assistance Center.
- Interface up or down transitions and system restart messages, displayed at the notifications level. This message is only for information; switch functionality is not affected.
Limiting Syslog Messages Sent to the History Table and to SNMP

If you enabled syslog message traps to be sent to an SNMP network management station by using the `snmp-server enable trap` global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level `warning` and numerically lower levels (see Table 30-3 on page 30-9) are stored in the history table even if syslog traps are not enabled.

Beginning in privileged EXEC mode, follow these steps to change the level and history table size defaults. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 logging history level</td>
<td>Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 30-3 on page 30-9 for a list of level keywords. By default, <code>warnings</code>, <code>errors</code>, <code>critical</code>, <code>alerts</code>, and <code>emergencies</code> messages are sent.</td>
</tr>
<tr>
<td>Step 3 logging history size</td>
<td>Specify the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 0 to 500 messages.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

When the history table is full (it contains the maximum number of message entries specified with the `logging history size` global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the `no logging history` global configuration command. To return the number of messages in the history table to the default value, use the `no logging history size` global configuration command.

Enabling the Configuration-Change Logger

You can enable a configuration logger to keep track of configuration changes made with the command-line interface (CLI). When you enter the `logging enable` configuration-change logger configuration command, the log records the session, the user, and the command that was entered to change the configuration. You can configure the size of the configuration log from 1 to 1000 entries (the default is 100). You can clear the log at any time by entering the `no logging enable` command followed by the `logging enable` command to disable and reenable logging.
Use the `show archive log config {all | number [end-number] | user username [session number] number [end-number] | statistics} [provisioning]` privileged EXEC command to display the complete configuration log or the log for specified parameters.

The default is that configuration logging is disabled.

For information about the commands, see the *Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T:*


Beginning in privileged EXEC mode, follow these steps to enable configuration logging:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>archive</strong> Enter archive configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>log config</strong> Enter configuration-change logger configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>logging enable</strong> Enable configuration change logging.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>logging size entries</strong> <em>(Optional) Configure the number of entries retained in the configuration log. The range is from 1 to 1000. The default is 100.</em></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>show archive log config</strong> Verify your entries by viewing the configuration log.</td>
</tr>
</tbody>
</table>

This example shows how to enable the configuration-change logger and to set the number of entries in the log to 500.

Switch(config)# archive
Switch(config-archive)# log config
Switch(config-archive-log-cfg)# logging enable
Switch(config-archive-log-cfg)# logging size 500
Switch(config-archive-log-cfg)# end

This is an example of output for the configuration log:

Switch# `show archive log config all`

```
idx | sess | user@line       | Logged command                                           |
38  | 11   | unknown user@vty3 | no aaa authorization config-commands                      |
39  | 12   | unknown user@vty3 | no aaa authorization network default group radius         |
40  | 12   | unknown user@vty3 | no aaa accounting dot1x default start-stop group radius   |
41  | 13   | unknown user@vty3 | no aaa accounting system default                          |
42  | 14   | temi@vty4         | interface GigabitEthernet4/0/1                           |
43  | 14   | temi@vty4         | switchport mode trunk                                    |
44  | 14   | temi@vty4         | exit                                                      |
45  | 16   | temi@vty5         | interface FastEthernet5/0/1                              |
46  | 16   | temi@vty5         | switchport mode trunk                                    |
47  | 16   | temi@vty5         | exit                                                      |
```

### Configuring UNIX Syslog Servers

The next sections describe how to configure the UNIX server syslog daemon and how to define the UNIX system logging facility.
Logging Messages to a UNIX Syslog Daemon

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. This procedure is optional.

Log in as root, and perform these steps:

**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.

---

**Step 1**

Add a line such as the following to the file `/etc/syslog.conf`:

```
local7.debug /usr/adm/logs/cisco.log
```

The `local7` keyword specifies the logging facility to be used; see Table 30-4 on page 30-13 for information on the facilities. The `debug` keyword specifies the syslog level; see Table 30-3 on page 30-9 for information on the severity levels. The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

**Step 2**

Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /var/log/cisco.log
$ chmod 666 /var/log/cisco.log
```

**Step 3**

Make sure the syslog daemon reads the new changes:

```
$ kill -HUP `cat /etc/syslog.pid`
```

For more information, see the `man syslog.conf` and `man syslogd` commands on your UNIX system.

---

Configuring the UNIX System Logging Facility

When sending system log messages to an external device, you can cause the switch to identify its messages as originating from any of the UNIX syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure UNIX system facility message logging. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>logging <code>host</code></td>
</tr>
<tr>
<td></td>
<td>Log messages to a UNIX syslog server host by entering its IP address.</td>
</tr>
<tr>
<td></td>
<td>To build a list of syslog servers that receive logging messages, enter</td>
</tr>
<tr>
<td></td>
<td>this command more than once.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>logging trap <code>level</code></td>
</tr>
<tr>
<td></td>
<td>Limit messages logged to the syslog servers.</td>
</tr>
<tr>
<td></td>
<td>Be default, syslog servers receive informational messages and lower.</td>
</tr>
<tr>
<td></td>
<td>See Table 30-3 on page 30-9 for <code>level</code> keywords.</td>
</tr>
</tbody>
</table>
To remove a syslog server, use the `no logging host` global configuration command, and specify the syslog server IP address. To disable logging to syslog servers, enter the `no logging trap` global configuration command.

Table 30-4 lists the UNIX system facilities supported by the software. For more information about these facilities, consult the operator’s manual for your UNIX operating system.

### Table 30-4 Logging Facility-Type Keywords

<table>
<thead>
<tr>
<th>Facility Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>Authorization system</td>
</tr>
<tr>
<td>cron</td>
<td>Cron facility</td>
</tr>
<tr>
<td>daemon</td>
<td>System daemon</td>
</tr>
<tr>
<td>kern</td>
<td>Kernel</td>
</tr>
<tr>
<td>local0-7</td>
<td>Locally defined messages</td>
</tr>
<tr>
<td>lpr</td>
<td>Line printer system</td>
</tr>
<tr>
<td>mail</td>
<td>Mail system</td>
</tr>
<tr>
<td>news</td>
<td>USENET news</td>
</tr>
<tr>
<td>sys9-14</td>
<td>System use</td>
</tr>
<tr>
<td>syslog</td>
<td>System log</td>
</tr>
<tr>
<td>user</td>
<td>User process</td>
</tr>
<tr>
<td>uucp</td>
<td>UNIX-to-UNIX copy system</td>
</tr>
</tbody>
</table>

### Displaying the Logging Configuration

To display the logging configuration and the contents of the log buffer, use the `show logging` privileged EXEC command. For information about the fields in this display, see the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.
Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Catalyst 3560 switch.

Note


- Understanding SNMP, page 31-1
- Configuring SNMP, page 31-6
- Displaying SNMP Status, page 31-18

Understanding SNMP

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 MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. 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.

These sections contain this conceptual information:

- SNMP Versions, page 31-2
- SNMP Manager Functions, page 31-3
- SNMP Agent Functions, page 31-4
- SNMP Community Strings, page 31-4
- Using SNMP to Access MIB Variables, page 31-4
SNMP Versions

This software release supports these 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—ensuring that a packet was not tampered with in transit
  - Authentication—determining that the message is from a valid source
  - Encryption—mixing the contents of a package to prevent it from being read by an unauthorized source.

Note: To select encryption, enter the `priv` keyword. This keyword is available only when the cryptographic (encrypted) software image is installed.

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 mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism 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 mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

Table 31-1 identifies the characteristics of the 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>
</tbody>
</table>
Understanding SNMP

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.

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 31-2.

<table>
<thead>
<tr>
<th>Table 31-2</th>
<th>SNMP Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation</strong></td>
<td><strong>Description</strong></td>
</tr>
<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.¹</td>
</tr>
<tr>
<td>get-bulk-request²</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>

1. 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.

2. 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 these attributes:

- Read-only (RO)—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write (RW)—Gives read and write access to authorized management stations to all objects in the MIB, 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. For more information, see Chapter 5, “Clustering Switches” and see Getting Started with Cisco Network Assistant, available on Cisco.com.

Using SNMP to Access MIB Variables

An example of an NMS is the CiscoWorks network management software. CiscoWorks 2000 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 Figure 31-1, 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 re-sent, 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 re-sent 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 Table 31-3 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(^1)</td>
<td>1–4999</td>
</tr>
<tr>
<td>EtherChannel</td>
<td>5000–5012</td>
</tr>
<tr>
<td>Loopback</td>
<td>5013–5077</td>
</tr>
</tbody>
</table>
Table 31-3  ifIndex Values (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>ifIndex Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel</td>
<td>5078–5142</td>
</tr>
<tr>
<td>Physical (such as Gigabit Ethernet or SFP²-module interfaces)</td>
<td>10000–14500</td>
</tr>
<tr>
<td>Null</td>
<td>14501</td>
</tr>
</tbody>
</table>

1. SVI = switch virtual interface
2. SFP = small form-factor pluggable

Note

The switch might not use sequential values within a range.

### Configuring SNMP

- Default SNMP Configuration, page 31-6
- SNMP Configuration Guidelines, page 31-7
- Disabling the SNMP Agent, page 31-7
- Configuring Community Strings, page 31-8
- Configuring SNMP Groups and Users, page 31-9
- Configuring SNMP Notifications, page 31-12
- Setting the CPU Threshold Notification Types and Values, page 31-15
- Setting the Agent Contact and Location Information, page 31-16
- Limiting TFTP Servers Used Through SNMP, page 31-16
- SNMP Examples, page 31-17

### Default SNMP Configuration

Table 31-4 shows the default SNMP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP agent</td>
<td>Disabled¹.</td>
</tr>
<tr>
<td>SNMP trap receiver</td>
<td>None configured.</td>
</tr>
<tr>
<td>SNMP traps</td>
<td>None enabled except the trap for TCP connections (tty).</td>
</tr>
<tr>
<td>SNMP version</td>
<td>If no version keyword is present, the default is Version 1.</td>
</tr>
<tr>
<td>SNMPv3 authentication</td>
<td>If no keyword is entered, the default is the noauth (noAuthNoPriv) security level.</td>
</tr>
<tr>
<td>SNMP notification type</td>
<td>If no type is specified, all notifications are sent.</td>
</tr>
</tbody>
</table>

1. 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 autogenerates 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. See the *Cisco IOS Network Management Command Reference* for information about when you should configure notify views.
- 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 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 important side effects. 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.

Disabling the SNMP Agent

Beginning in privileged EXEC mode, follow these steps to disable the SNMP agent:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 no snmp-server</td>
<td>Disable the SNMP agent operation.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

The `no snmp-server` global configuration command disables all running versions (Version 1, Version 2C, and Version 3) on the device. No specific Cisco IOS command exists to enable SNMP. The first `snmp-server` global configuration command that you enter enables all versions of SNMP.
## 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

Beginning in privileged EXEC mode, follow these steps to configure a community string on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`snmp-server community string [view view-name] [ro</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><strong>Step 3</strong></td>
<td>`access-list access-list-number [deny</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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>end</code></td>
</tr>
</tbody>
</table>
### Configuring SNMP

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).

To remove a specific community string, use the `no snmp-server community string` global configuration command.

This example shows how to assign the string `comaccess` to SNMP, to allow read-only access, and to specify that IP access list 4 can use the community string to gain access to the switch SNMP agent:

```
Switch(config)# snmp-server community comaccess ro 4
```

### 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.

Beginning in privileged EXEC mode, follow these steps to configure SNMP on the switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
**configure terminal**  |  Enter global configuration mode.  |
| **Step 2**  |  
**snmp-server engineID**  |  Configure a name for either the local or remote copy of SNMP.  |
|  |  |  • 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. For example, to configure an engine ID of 123400000000000000000000, you can enter this: `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 3

**Command**

```
snmp-server group groupname {v1 | v2c | v3
{auth | noauth | priv}} [read readview]
[write writeview] [notify notifyview] [access
access-list]
```

**Purpose**

Configure a new SNMP group on the remote device.

- For `groupname`, specify the name of the group.
- Specify a security model:
  - `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 an authentication level:
    - `auth`—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication.
    - `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`).

**Note**

The `priv` keyword is available only when the cryptographic software image is installed.

- (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 4

```
snmp-server user username groupname
topic 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]
```

**Purpose**
Add a new user for an SNMP group.

- The `username` is the name of the user on the host that connects to the agent.
- The `groupname` 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` and the switch is running the cryptographic software image, you can also configure a private (`priv`) encryption algorithm and password string `priv-password` (not to exceed 64 characters).
    - `priv` specifies the User-based Security Model (USM).
    - `des` specifies the use of the 56-bit DES algorithm.
    - `3des` specifies the use of the 168-bit DES algorithm.
    - `aes` specifies the use of the DES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.
  - (Optional) Enter `access access-list` with a string (not to exceed 64 characters) that is the name of the access list.

### Step 5
```
end
```

**Purpose**
Return to privileged EXEC mode.

### Step 6
```
show running-config
```

**Purpose**
Verify your entries.

**Note**
To display SNMPv3 information about `auth` | `noauth` | `priv` mode configuration, you must enter the `show snmp user` privileged EXEC command.

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

**Purpose**
(Optional) Save your entries in the configuration file.
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.

Table 31-5 describes the supported switch traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them. To enable the sending of SNMP inform notifications, use the `snmp-server enable traps` global configuration command combined with the `snmp-server host host-addr informs` global configuration command.

<table>
<thead>
<tr>
<th>Notification Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Generates Border Gateway Protocol (BGP) state change traps. This option is only available when the enhanced multilayer image is installed.</td>
</tr>
<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>entity</td>
<td>Generates a trap for SNMP entity changes.</td>
</tr>
<tr>
<td>cpu threshold</td>
<td>Allow CPU-related traps.</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 erdisabled. 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.</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>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>
Chapter 31  Configuring SNMP

Table 31-5  Switch Notification Types (continued)

<table>
<thead>
<tr>
<th>Notification Type Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-security</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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:

- `snmp-server enable traps port-security`
- `snmp-server enable traps port-security trap-rate rate`

<table>
<thead>
<tr>
<th>rtr</th>
<th>Generates a trap for the SNMP Response Time Reporter (RTR).</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp</td>
<td>Generates a trap for SNMP-type notifications for authentication, cold start, warm start, link up or link down.</td>
</tr>
<tr>
<td>storm-control</td>
<td>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).</td>
</tr>
<tr>
<td>stpx</td>
<td>Generates SNMP STP Extended MIB traps.</td>
</tr>
<tr>
<td>syslog</td>
<td>Generates SNMP syslog traps.</td>
</tr>
<tr>
<td>tty</td>
<td>Generates a trap for TCP connections. This trap is enabled by default.</td>
</tr>
<tr>
<td>vlan-membership</td>
<td>Generates a trap for SNMP VLAN membership changes.</td>
</tr>
<tr>
<td>vlancreate</td>
<td>Generates SNMP VLAN created traps.</td>
</tr>
<tr>
<td>vlandelete</td>
<td>Generates SNMP VLAN deleted traps.</td>
</tr>
<tr>
<td>vtp</td>
<td>Generates a trap for VLAN Trunking Protocol (VTP) changes.</td>
</tr>
</tbody>
</table>

**Note**  Though visible in the command-line help strings, the **fru-ctrl, insertion, and removal** keywords are not supported.

You can use the `snmp-server host` global configuration command to a specific host to receive the notification types listed in Table 31-5.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send traps or informs to a host:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>snmp-server engineID remote ip-address engineid-string</code></td>
<td>Specify the engine ID for the remote host.</td>
</tr>
<tr>
<td></td>
<td>`snmp-server user username groupname {remote host udp-port port} {v1 [access access-list]</td>
<td>v2c [access access-list]</td>
</tr>
</tbody>
</table>

**Note**  You cannot configure a remote user for an address without first configuring the engine ID for the remote host. Otherwise, you receive an error message, and the command is not executed.
## Chapter 31  Configuring SNMP

### Command

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snmp-server group</strong></td>
<td><strong>groupname</strong></td>
<td>Configure an SNMP group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snmp-server host</strong></td>
<td><strong>host-addr</strong> [<strong>informs</strong></td>
<td>Specify the recipient of an SNMP trap operation.</td>
</tr>
</tbody>
</table>

- For **host-addr**, specify the name or Internet address of the host (the targeted recipient).
- (Optional) Enter **informs** to send SNMP informs to the host.
- (Optional) Enter **traps** (the default) to send SNMP traps to the host.
- (Optional) Specify the SNMP **version** (1, 2c, or 3). SNMPv1 does not support informs.
- (Optional) For Version 3, select authentication level **auth**, **noauth**, or **priv**. |

**Note** The **priv** keyword is available only when the cryptographic software image is installed.

- For **community-string**, when **version 1** or **version 2c** is specified, enter the password-like community string sent with the notification operation. When **version 3** is specified, enter the SNMPv3 username. |

**Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

- (Optional) For **notification-type**, use the keywords listed in Table 31-5 on page 31-12. If no type is specified, all notifications are sent. |

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snmp-server enable traps</strong></td>
<td><strong>notification-types</strong></td>
<td>Enable the switch to send traps or informs and specify the type of notifications to be sent. For a list of notification types, see Table 31-5 on page 31-12, or enter <strong>snmp-server enable traps</strong>?</td>
</tr>
</tbody>
</table>

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:

- **snmp-server enable traps port-security** |
- **snmp-server enable traps port-security trap-rate** |

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snmp-server trap-source</strong></td>
<td><strong>interface-id</strong></td>
<td>(Optional) Specify the source interface, which provides the IP address for the trap message. This command also sets the source IP address for informs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snmp-server queue-length</strong></td>
<td><strong>length</strong></td>
<td>(Optional) Establish the message queue length for each trap host. The range is 1 to 1000; the default is 10.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>snmp-server trap-timeout</strong></td>
<td><strong>seconds</strong></td>
<td>(Optional) Define how often to resend trap messages. The range is 1 to 1000; the default is 30 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>end</strong></td>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
The `snmp-server host` command specifies which hosts receive the notifications. The `snmp-server enable trap` command globally enables the mechanism 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` 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 CPU Threshold Notification Types and Values

Beginning in privileged EXEC mode, follow these steps to set the CPU threshold notification types and values:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | process cpu threshold type { total | process | interrupt } rising percentage interval seconds [ falling fall-percentage interval seconds ] | Set the CPU threshold notification types and values:

- **total**—set the notification type to total CPU utilization.
- **process**—set the notification type to CPU process utilization.
- **interrupt**—set the notification type to CPU interrupt utilization.
- **rising percentage**—the percentage (1 to 100) of CPU resources that, when exceeded for the configured interval, sends a CPU threshold notification.
- **interval seconds**—the duration of the CPU threshold violation in seconds (5 to 86400) that, when met, sends a CPU threshold notification.
- **falling fall-percentage**—the percentage (1 to 100) of CPU resources that, when usage falls below this level for the configured interval, sends a CPU threshold notification.

This value must be equal to or less than the **rising percentage** value. If not specified, the **falling fall-percentage** value is the same as the **rising percentage** value. |
| **Step 3** | end | Return to privileged EXEC mode. |
| **Step 4** | show running-config | Verify your entries. |
| **Step 5** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |
Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp-server contact text</td>
</tr>
<tr>
<td>Step 3</td>
<td>snmp-server location text</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Limiting TFTP Servers Used Through SNMP

Beginning in privileged EXEC mode, 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>snmp-server tftp-server-list access-list-number</td>
</tr>
</tbody>
</table>
| Step 3 | access-list access-list-number {deny | permit} source [source-wildcard] | Create a standard access list, repeating the command as many times as necessary.  
- For access-list-number, enter the access list number specified in Step 2.  
- 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. Recall that the access list is always terminated by an implicit deny statement for everything. |
### 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
```

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Displaying 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 in Table 31-6 to display SNMP information. For information about the fields in the displays, see the *Cisco IOS Configuration Fundamentals Command Reference*.

**Table 31-6 Commands for Displaying SNMP Information**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show snmp</code></td>
<td>Displays SNMP statistics.</td>
</tr>
<tr>
<td>`show snmp engineID [local</td>
<td>remote]`</td>
</tr>
<tr>
<td><code>show snmp group</code></td>
<td>Displays information on each SNMP group on the network.</td>
</tr>
<tr>
<td><code>show snmp pending</code></td>
<td>Displays information on pending SNMP requests.</td>
</tr>
<tr>
<td><code>show snmp sessions</code></td>
<td>Displays information on the current SNMP sessions.</td>
</tr>
<tr>
<td><code>show snmp user</code></td>
<td>Displays information on each SNMP user name in the SNMP users table.</td>
</tr>
</tbody>
</table>

**Note** You must use this command to display SNMPv3 configuration information for `auth | noauth | priv` mode. This information is not displayed in the `show running-config` output.
CHAPTER 32

Configuring Embedded Event Manager

Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery within a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any other EEM action when the monitored events occur or when a threshold is reached. An EEM policy defines an event and the actions to be taken when that event occurs.

This chapter tells how to use EEM and how to configure it on the Catalyst 3560 switch. For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the Cisco IOS Network Management Command Reference. For the complete EEM document set, see these documents in the Cisco IOS Network Management Configuration Guide:


Note
Beginning with Cisco IOS Release 12.2(55)SE, this feature is supported on switches running the IP base image.

This chapter has these sections:

- Understanding Embedded Event Manager, page 32-1
- Configuring Embedded Event Manager, page 32-5
- Displaying Embedded Event Manager Information, page 32-7

Understanding Embedded Event Manager

EEM monitors key system events and then acts on them through a set policy. This policy is a programmed script that you can use to customize a script to invoke an action based on a given set of events occurring. The script generates actions such as generating custom syslog or Simple Network Management Protocol (SNMP) traps, invoking CLI commands, forcing a failover, and so forth. The event management capabilities of EEM are useful because not all event management can be managed from the switch and because some problems compromise communication between the switch and the external network management device. Network availability is improved if automatic recovery actions are performed without rebooting the switch.
Figure 32-1 shows the relationship between the EEM server, the core event publishers (event detectors), and the event subscribers (policies). The event publishers screen events and publish them when there is a match on an event specification that is provided by the event subscriber. Event detectors notify the EEM server when an event occurs. The EEM policies then implement recovery based on the current state of the system and the actions specified in the policy for the given event.

Event Detectors

EEM software programs known as event detectors determine when an EEM event occurs. Event detectors are separate systems that provide an interface between the agent being monitored, for example SNMP, and the EEM policies where an action can be implemented.

- Application-specific event detector—Allows any EEM policy to publish an event.
- IOS CLI event detector—Generates policies based on the commands entered through the CLI.

See the *EEM Configuration for Cisco Integrated Services Router Platforms Guide* for examples of EEM deployment.

- Event Detectors, page 32-2
- Embedded Event Manager Actions, page 32-4
- Embedded Event Manager Policies, page 32-4
- Embedded Event Manager Environment Variables, page 32-4
- EEM 3.2, page 32-5
• Generic Online Diagnostics (GOLD) event detector—Publishes an event when a GOLD failure event is detected on a specified card and subcard.

• Counter event detector—Publishes an event when a named counter crosses a specified threshold.

• Interface counter event detector—Publishes an event when a generic Cisco IOS interface counter for a specified interface crosses a defined threshold. A threshold can be specified as an absolute value or an incremental value. For example, if the incremental value is set to 50 an event would be published when the interface counter increases by 50.

This detector also publishes an event about an interface based on the rate of change for the entry and exit values.

• None event detector—Publishes an event when the event manager run CLI command executes an EEM policy. EEM schedules and runs policies on the basis on an event specification within the policy itself. An EEM policy must be manually identified and registered before the event manager run command executes.

• Online insertion and removal event detector—Publishes an event when a hardware insertion or removal (OIR) event occurs.

• Resource threshold event detector—Generates policies based on global platform values and thresholds. Includes resources such as CPU utilization and remaining buffer capacity.

• Remote procedure call (RPC) event detector—Invokes EEM policies from outside the switch over an encrypted connecting using Secure Shell (SSH) and uses Simple Object Access Protocol (SOAP) data encoding for exchanging XML-based messages. It also runs EEM policies and then gets the output in a SOAP XML-formatted reply.

• SNMP event detector—Allows a standard SNMP MIB object to be monitored and an event to be generated when
  – The object matches specified values or crosses specified thresholds.
  – The SNMP delta value, the difference between the monitored Object Identifier (OID) value at the beginning the period and the actual OID value when the event is published, matches a specified value.

• SNMP notification event detector—Intercepts SNMP trap and inform messages received by the switch. The event is generated when an incoming message matches a specified value or crosses a defined threshold.

• Syslog event detector—Allows for screening syslog messages for a regular expression pattern match. The selected messages can be further qualified, requiring that a specific number of occurrences be logged within a specified time. A match on a specified event criteria triggers a configured policy action.

• Timer event detector—Publishes events for
  – An absolute-time-of-day timer publishes an event when a specified absolute date and time occurs.
  – A countdown timer publishes an event when a timer counts down to zero.
  – A watchdog timer publishes an event when a timer counts down to zero. The timer automatically resets itself to its initial value and starts to count down again.
  – A CRON timer publishes an event by using a UNIX standard CRON specification to define when the event is to be published. A CRON timer never publishes events more than once per minute.
• Watchdog event detector (IOSWDSysMon)—Publishes an event when
  – CPU utilization for a Cisco IOS process crosses a threshold.
  – Memory utilization for a Cisco IOS process crosses a threshold.

Two events can be monitored at the same time, and the event publishing criteria requires that one or both events cross their specified thresholds.

**Embedded Event Manager Actions**

These actions occur in response to an event:

• Modifying a named counter.
• Publishing an application-specific event.
• Generating an SNMP trap.
• Generating prioritized syslog messages.
• Reloading the Cisco IOS software.

**Embedded Event Manager Policies**

EEM can monitor events and provide information, or take corrective action when the monitored events occur or a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

There are two types of EEM policies: an applet or a script. An applet is a simple policy that is defined within the CLI configuration. It is a concise method for defining event screening criteria and the actions to be taken when that event occurs. Scripts are defined on the networking device by using an ASCII editor. The script, which can be a bytecode (.tbc) and text (.tcl) script, is then copied to the networking device and registered with EEM. You can also register multiple events in a .tcl file.

You use EEM to write and implement your own policies using the EEM policy tool command language (TCL) script.

Cisco enhancements to TCL in the form of keyword extensions facilitate the development of EEM policies. These keywords identify the detected event, the subsequent action, utility information, counter values, and system information.

For complete information on configuring EEM policies and scripts, see the *Cisco IOS Network Management Configuration Guide, Release 12.4T*.

**Embedded Event Manager Environment Variables**

EEM uses environment variables in EEM policies. These variables are defined in a EEM policy tool command language (TCL) script by running a CLI command and the `event manager environment` command.

• User-defined variables
  Defined by the user for a user-defined policy.
• Cisco-defined variables
  Defined by Cisco for a specific sample policy.
Cisco built-in variables (available in EEM applets)

Defined by Cisco and can be read-only or read-write. The read-only variables are set by the system before an applet starts to execute. The single read-write variable, _exit_status, allows you to set the exit status for policies triggered from synchronous events.

Cisco-defined environment variables and Cisco system-defined environment variables might apply to one specific event detector or to all event detectors. Environment variables that are user-defined or defined by Cisco in a sample policy are set by using the event manager environment global configuration command. You must defined the variables in the EEM policy before you register the policy.

For information about the environmental variables that EEM supports, see the Cisco IOS Network Management Configuration Guide, Release 12.4T.

EEM 3.2

EEM 3.2 is supported in Cisco IOS Release 12.2(52)SE and later and introduces these event detectors:

- Neighbor Discovery—Neighbor Discovery event detector provides the ability to publish a policy to respond to automatic neighbor detection when:
  - a Cisco Discovery Protocol (CDP) cache entry is added, deleted, or updated.
  - a Link Layer Discovery Protocol (LLDP) cache entry is added, deleted or updated.
  - an interface link status changes.
  - an interface line status changes.
- Identity—Identity event detector generates an event when AAA authorization and authentication is successful, when failure occurs, or after normal user traffic on the port is allowed to flow.
- Mac-Address-Table—Mac-Address-Table event detector generates an event when a MAC address is learned in the MAC address table.

Note

The Mac-Address-Table event detector is supported only on switch platforms and can be used only on Layer 2 interfaces where MAC addresses are learned. Layer 3 interfaces do not learn addresses routers do not usually support the MAC address-table infrastructure needed to notify EEM of a learned MAC address.

EEM 3.2 also introduces CLI commands to support the applets to work with the new event detectors.

For details about EEM 3.2 features, see the Embedded Event Manager 3.2 document:

Configuring Embedded Event Manager

- Registering and Defining an Embedded Event Manager Applet, page 32-6
- Registering and Defining an Embedded Event Manager TCL Script, page 32-6

For complete information about configuring embedded event manager, see the Cisco IOS Network Management Configuration Guide, Release 12.4T.
Registering and Defining an Embedded Event Manager Applet

Beginning in privileged EXEC mode, perform this task to register an applet with EEM and to define the EEM applet using the event applet and action applet configuration commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>event manager applet applet-name</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>event snmp oid oid-value get-type [exact</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>action label syslog [priority priority-level] msg msg-text</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
</tbody>
</table>

This example shows the output for EEM when one of the fields specified by an SNMP object ID crosses a defined threshold:

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.6.1 get-type exact entry-op lt entry-val 5120000 poll-interval 10
```

These examples show actions that are taken in response to an EEM event:

```
Switch(config-applet)# action 1.0 syslog priority critical msg "Memory exhausted; current available memory is $snmp_oid_val bytes"
Switch(config-applet)# action 2.0 force-switchover
```

Registering and Defining an Embedded Event Manager TCL Script

Beginning in privileged EXEC mode, perform this task to register a TCL script with EEM and to define the TCL script and policy commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>show event manager environment [all</td>
</tr>
</tbody>
</table>

This example shows the output for EEM when one of the fields specified by an SNMP object ID crosses a defined threshold:

```
Switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.48.1.1.6.1 get-type exact entry-op lt entry-val 5120000 poll-interval 10
```
### Displaying Embedded Event Manager Information

To display information about EEM, including EEM registered policies and EEM history data, see the Cisco IOS Network Management Command Reference.
This chapter describes how to configure network security on the Catalyst 3560 switch by using access control lists (ACLs), also referred to as access lists. In this chapter, references to IP ACLs are specific to IP Version 4 (IPv4) ACLs. For information about IPv6 ACLs, see Chapter 40, “Configuring IPv6 ACLs.”

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release, the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the Cisco IOS IP Configuration Guide, Release 12.2, and the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2. The Cisco IOS documentation is available from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides or Command References.

The switch also supports Cisco TrustSec Security Group Tag (SCT) Exchange Protocol (SXP). This feature supports security group access control lists (SGACLs), which define ACL policies for a group of devices instead of an IP address. The SXP control protocol allows tagging packets with SCTs without a hardware upgrade, and runs between access layer devices at the Cisco TrustSec domain edge and distribution layer devices within the Cisco TrustSec domain. Catalyst 3560 switches operate as access layer switches in the Cisco TrustSec network.

For more information about Cisco TrustSec, see the Cisco TrustSec Switch Configuration Guide: http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

The sections on SXP define the capabilities supported on the Catalyst 3560 switch.

- Understanding ACLs, page 33-1
- Configuring IPv4 ACLs, page 33-6
- Creating Named MAC Extended ACLs, page 33-27
- Configuring VLAN Maps, page 33-29
- Using VLAN Maps with Router ACLs, page 33-36
- Displaying IPv4 ACL Configuration, page 33-41

**Understanding ACLs**

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
Understanding ACLs

The switch supports both IP 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.

This switch also supports quality of service (QoS) classification ACLs. For more information, see the “Classification Based on QoS ACLs” section on page 34-8.

These sections contain this conceptual information:

- [Supported ACLs](#)
- [Handling Fragmented and Unfragmented Traffic](#)

### Supported ACLs

- **Port ACLs** access-control traffic entering a Layer 2 interface. The switch does not support port ACLs in the outbound direction. You can apply only one IP access list and one MAC access list to a Layer 2 interface. For more information, see the “Port ACLs” section on page 33-3.

- **Router ACLs** access-control routed traffic between VLANs and are applied to Layer 3 interfaces in a specific direction (inbound or outbound). For more information, see the “Router ACLs” section on page 33-4.

- **VLAN ACLs** or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access control based on Layer 3 addresses for IPv4. Unsupported protocols are access-controlled through MAC addresses using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port after being routed. For more information, see the “VLAN Maps” section on page 33-5.
You can use input port ACLs, router ACLs, and VLAN maps on the same switch. However, a port ACL takes precedence over a router ACL or VLAN map.

- When both an input port ACL and a VLAN map are applied, incoming packets received on ports with a port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.
- When an input router ACL and input port ACL exist in a switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.
- When a VLAN map, input router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.
- When a VLAN map, output router ACL, and input port ACL exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Outgoing routed IP packets are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.

If IEEE 802.1Q tunneling is configured on an interface, any IEEE 802.1Q encapsulated IP packets received on the tunnel port can be filtered by MAC ACLs, but not by IP ACLs. This is because the switch does not recognize the protocol inside the IEEE 802.1Q header. This restriction applies to router ACLs, port ACLs, and VLAN maps. For more information about IEEE 802.1Q tunneling, see Chapter 16, “Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling.”

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 and can be applied only on interfaces in the inbound direction. These 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 associated with all inbound features configured on a given 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 33-1 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.
Understanding ACLs

When you apply a port ACL to a trunk port, the ACL filters traffic on all VLANs present on the trunk port. When you apply a port ACL to a port with voice VLAN, the ACL filters traffic on both data and voice VLANs.

With port ACLs, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC addresses. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP access list and a MAC access list to the interface.

Note

You cannot apply more than one IP access list and one MAC access list to a Layer 2 interface. If an IP access list or MAC access list is already configured on a Layer 2 interface and you apply a new IP access list or MAC access list to the interface, the new ACL replaces the previously configured one.

Router ACLs

You can apply router ACLs on switch virtual interfaces (SVIs), which are Layer 3 interfaces to VLANs; on physical Layer 3 interfaces; and on Layer 3 EtherChannel interfaces. You apply router ACLs on interfaces for specific directions (inbound or outbound). You can apply one router ACL in each direction on an interface.

An ACL can be used with multiple features for a given interface, and one feature can use multiple ACLs. When a single router ACL is used by multiple features, it is examined multiple times.

Supported access lists for IPv4 traffic:

- Standard IP access lists use source addresses for matching operations.
- Extended IP access lists use source and destination addresses and optional protocol information for matching operations.
As with port ACLs, the switch examines ACLs associated with features configured on a given interface. However, you can apply only inbound port ACLs, while router ACLs are supported in both directions. As packets enter the switch on an interface, ACLs associated with all inbound features configured on that interface are examined. After packets are routed and before they are forwarded to the next hop, all ACLs associated with outbound features configured on the egress interface are examined.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL and can be used to control access to a network or to part of a network. In Figure 33-1, ACLs applied at the router input allow Host A to access the Human Resources network but prevent Host B from accessing the same network.

**VLAN Maps**

Use VLAN ACLs or VLAN maps to access-control all traffic. You can apply VLAN maps to all packets that are routed into or out of a VLAN or are bridged within a VLAN in the switch.

Use VLAN maps for security packet filtering. VLAN maps are not defined by direction (input or output).

You can configure VLAN maps to match Layer 3 addresses for IPv4 traffic.

All non-IP protocols are access-controlled through MAC addresses and Ethertype using MAC VLAN maps. (IP traffic is not access controlled by MAC VLAN maps.) You can enforce VLAN maps only on packets going through the switch; you cannot enforce VLAN maps on traffic between hosts on a hub or on another switch connected to this switch.

With VLAN maps, forwarding of packets is permitted or denied, based on the action specified in the map. Figure 33-2 shows how a VLAN map is applied to prevent a specific type of traffic from Host A in VLAN 10 from being forwarded. You can apply only one VLAN map to a VLAN.

**Handling 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 ACEs do not check Layer 4 information and therefore can be applied to all packet fragments. ACEs that do test Layer 4 information cannot be applied in the standard manner to most of the fragments in a fragmented IP packet. When the fragment contains no Layer 4 information and the ACE tests some Layer 4 information, the matching rules are modified:

- Permit ACEs that check the Layer 3 information in the fragment (including protocol type, such as TCP, UDP, and so on) are considered to match the fragment regardless of what the missing Layer 4 information might have been.
• Deny ACEs that check Layer 4 information never match a fragment unless the fragment contains Layer 4 information.

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 \textit{eq} keyword after the destination address means to test for the TCP-destination-port well-known numbers equaling Simple Mail Transfer Protocol (SMTP) and Telnet, respectively.

• Packet A is a TCP packet from host 10.2.2.2, port 65000, going to host 10.1.1.1 on the SMTP port. If this packet is fragmented, the first fragment matches the first ACE (a permit) as if it were a complete packet because all Layer 4 information is present. The remaining fragments also match the first ACE, even though they do not contain the SMTP port information, because the first ACE only checks Layer 3 information when applied to fragments. The information in this example is that the packet is TCP and that the destination is 10.1.1.1.

• Packet B is from host 10.2.2.2, port 65001, going to host 10.1.1.2 on the Telnet port. If this packet is fragmented, the first fragment matches the second ACE (a deny) because all Layer 3 and Layer 4 information is present. The remaining fragments in the packet do not match the second ACE because they are missing Layer 4 information. Instead, they match the third ACE (a permit). Because the first fragment was denied, host 10.1.1.2 cannot reassemble a complete packet, so packet B is effectively denied. However, the later fragments that are permitted will consume bandwidth on the network and resources of host 10.1.1.2 as it tries to reassemble the packet.

• Fragmented packet C is from host 10.2.2.2, port 65001, going to host 10.1.1.3, port ftp. If this packet is fragmented, the first fragment matches the fourth ACE (a deny). All other fragments also match the fourth ACE because that ACE does not check any Layer 4 information and because Layer 3 information in all fragments shows that they are being sent to host 10.1.1.3, and the earlier permit ACEs were checking different hosts.

### Configuring IPv4 ACLs

Configuring IPv4 ACLs on the switch is the same as configuring IPv4 ACLs on other Cisco switches and routers. The process is briefly described here. For more detailed information on configuring ACLs, see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the Cisco IOS IP Configuration Guide, Release 12.2. For detailed information about the commands, see the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2. The Cisco IOS documentation is available from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides or Command References.

The switch does not support these Cisco IOS router ACL-related features:

- Non-IP protocol ACLs (see Table 33-1 on page 33-8) or bridge-group ACLs
- IP accounting
- Inbound and outbound rate limiting (except with QoS ACLs)
These are the steps to use IP ACLs on the switch:

**Step 1**
Create an ACL by specifying an access list number or name and the access conditions.

**Step 2**
Apply the ACL to interfaces or terminal lines. You can also apply standard and extended IP ACLs to VLAN maps.

These sections contain this configuration information:

- Creating Standard and Extended IPv4 ACLs, page 33-7
- Applying an IPv4 ACL to a Terminal Line, page 33-19
- Applying an IPv4 ACL to an Interface, page 33-19
- Hardware and Software Treatment of IP ACLs, page 33-21
- Troubleshooting ACLs, page 33-21
- IPv4 ACL Configuration Examples, page 33-22

### Creating 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.

These sections describe access lists and how to create them:

- Access List Numbers, page 33-8
- ACL Logging, page 33-8
- Creating a Numbered Standard ACL, page 33-9
- Creating a Numbered Extended ACL, page 33-10
- Resequencing ACEs in an ACL, page 33-14
- Creating Named Standard and Extended ACLs, page 33-14
- Using Time Ranges with ACLs, page 33-16
- Including Comments in ACLs, page 33-18
Access List Numbers

The number you use to denote your ACL shows the type of access list that you are creating. Table 33-1 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 33-1  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.

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.

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.

Creating a Numbered Standard ACL

Beginning in privileged EXEC mode, follow these steps to create a numbered standard ACL:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number [deny</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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show access-lists [number</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no access-list access-list-number global configuration command to delete the entire ACL. You cannot delete individual ACEs from numbered access lists.

**Note** 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.

This example shows how to create a standard ACL to deny access to IP host 171.69.198.102, permit access to any others, and display the results.

Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
  10 deny 171.69.198.102
  20 permit any

The switch always rewrites the order of standard access lists so that entries with host matches and entries with matches having a don’t care mask of 0.0.0.0 are moved to the top of the list, above any entries with non-zero don’t care masks. Therefore, in show command output and in the configuration file, the ACEs do not necessarily appear in the order in which they were entered.

After creating a numbered standard IPv4 ACL, you can apply it to terminal lines (see the “Applying an IPv4 ACL to a Terminal Line” section on page 33-19), to interfaces (see the “Applying an IPv4 ACL to an Interface” section on page 33-19), or to VLANs (see the “Configuring VLAN Maps” section on page 33-29).

Creating a Numbered Extended ACL

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.

Some protocols also have specific parameters and keywords that apply to that protocol. These IP protocols are supported (protocol keywords are in parentheses in bold):
- Authentication Header Protocol (ahp)
- Enhanced Interior Gateway Routing Protocol (eigrp)
- Encapsulation Security Payload (esp)
- 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).

**Note**  ICMP echo-reply cannot be filtered. All other ICMP codes or types can be filtered.

For more details on the specific keywords for each protocol, see these command references:
- Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2
- Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2

These documents are available from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

**Note**  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.

Supported parameters can be grouped into these categories: TCP, UDP, ICMP, IGMP, or other IP.
Beginning in privileged EXEC mode, follow these steps to create an extended ACL:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2a</td>
<td>access-list access-list-number {deny</td>
<td>permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</td>
</tr>
</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. |

Note This step includes options for most IP protocols. For additional specific parameters for TCP, UDP, ICMP, and IGMP, see steps 2b through 2e. 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), max-reliability (2), max-throughput (4), min-delay (8).
- log—Enter to create an informational logging message to be sent to the console about the packet that matches the entry or log-input to include the input interface in the log entry.
- time-range—For an explanation of this keyword, see the “Using Time Ranges with ACLs” section on page 33-16.
- dscp—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.
Chapter 33  Configuring Network Security with ACLs

### Configuring IPv4 ACLs

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list access-list-number</code> &lt;br&gt; `{deny</td>
<td>permit} protocol any any<code>&lt;br&gt;</code>[precedence precedence] [tos tos]<code>&lt;br&gt;</code>[fragments] [log] [log-input]<code>&lt;br&gt;</code>[time-range time-range-name]<code>&lt;br&gt;</code>[dscp dscp]`</td>
</tr>
<tr>
<td>or <code>access-list access-list-number</code> &lt;br&gt; `{deny</td>
<td>permit} protocol host host destination<code>&lt;br&gt;</code>[precedence precedence] [tos tos]<code>&lt;br&gt;</code>[fragments] [log] [log-input]<code>&lt;br&gt;</code>[time-range time-range-name]<code>&lt;br&gt;</code>[dscp dscp]`</td>
</tr>
</tbody>
</table>

**Step 2b**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number` <br> `{deny | permit} tcp source source-wildcard` <br> `[operator port] destination destination-wildcard` <br> `[operator port] [established]` <br> `[precedence precedence] [tos tos]` <br> `[fragments] [log] [log-input]` <br> `[time-range time-range-name]` <br> `[dscp dscp] [flag]` | (Optional) Define an extended TCP access list and the access conditions. Enter `tcp` for Transmission Control Protocol. The parameters are the same as those described in Step 2a, 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. To see TCP port names, use the `?` or see the “Configuring IP Services” section in the “IP Addressing and Services” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*. Use only TCP port numbers or names when filtering TCP. The other optional keywords have these meanings:  
- `established`—Enter to match an established connection. This has the same function as matching on the `ack` or `rst` flag.  
- `flag`—Enter one of these flags to match by the specified TCP header bits: `ack` (acknowledge), `fin` (finish), `psh` (push), `rst` (reset), `syn` (synchronize), or `urg` (urgent). |

**Step 2c**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list access-list-number</code> &lt;br&gt; `{deny</td>
<td>permit} udp source source-wildcard<code>&lt;br&gt;</code>[operator port] destination destination-wildcard<code>&lt;br&gt;</code>[operator port] [established]<code>&lt;br&gt;</code>[precedence precedence] [tos tos]<code>&lt;br&gt;</code>[fragments] [log] [log-input]<code>&lt;br&gt;</code>[time-range time-range-name]<code>&lt;br&gt;</code>[dscp dscp]`</td>
</tr>
</tbody>
</table>
### Chapter 33: Configuring Network Security with ACLs

#### Configuring IPv4 ACLs

**Step 2d**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number deny | permit | icmp source source-wildcard destination destination-wildcard [icmp-type | icmp-type icmp-code] | [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] | (Optional) Define an extended 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 2a, 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 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 `?`, or see the “Configuring IP Services” section of the Cisco IOS IP Configuration Guide, Release 12.2. |

**Step 2e**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `access-list access-list-number deny | permit | igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] | (Optional) Define an extended IGMP access list and the access conditions. Enter `igmp` for Internet Group Management Protocol. The IGMP parameters are the same as those described for most IP protocols in Step 2a, 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 3**

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

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show access-lists [number</td>
<td>name]`</td>
</tr>
</tbody>
</table>

**Step 5**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no access-list access-list-number` global configuration command to delete the entire access list. You cannot delete individual ACEs from numbered access lists.

This example shows how to create and display an extended access list to deny Telnet access from any host in network 171.69.198.0 to any host in network 172.20.52.0 and to permit any others. (The `eq` keyword after the destination address means to test for the TCP destination port number equaling Telnet.)

Switch(config)# `access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet`  
Switch(config)# `access-list 102 permit tcp any any`  
Switch(config)# `end`  
Switch# `show access-lists`  
Extended IP access list 102  
  10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet  
  20 permit tcp any any

After an ACL is created, any additions (possibly entered from the terminal) are placed at the end of the list. You cannot selectively add or remove access list entries from a numbered access list.

**Note**

When you are creating an ACL, remember that, by default, the end of the access list contains an implicit deny statement for all packets if it did not find a match before reaching the end.
After creating a numbered extended ACL, you can apply it to terminal lines (see the “Applying an IPv4 ACL to a Terminal Line” section on page 33-19), to interfaces (see the “Applying an IPv4 ACL to an Interface” section on page 33-19), or to VLANs (see the “Configuring VLAN Maps” section on page 33-29).

**Resequencing ACEs in an ACL**

Sequence numbers for the entries in an access list are automatically generated when you create a new ACL. You can use the `ip access-list resequence` global configuration command to edit the sequence numbers in an ACL and change the order in which ACEs are applied. For example, if you add a new ACE to an ACL, it is placed at the bottom of the list. By changing the sequence number, you can move the ACE to a different position in the ACL.

For information about the `ip access-list resequence` command:

**Creating Named Standard and Extended 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.

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; 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.

Consider these guidelines and limitations before configuring named ACLs:

- 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. VLAN maps also accept a name.
- A standard ACL and an extended ACL cannot have the same name.
- Numbered ACLs are also available, as described in the “Creating Standard and Extended IPv4 ACLs” section on page 33-7.
- You can use standard and extended ACLs (named or numbered) in VLAN maps.

Beginning in privileged EXEC mode, follow these steps to create a standard ACL using names:

<table>
<thead>
<tr>
<th>Command</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>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ip access-list standard name</code></td>
<td>Define a standard IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 1 to 99.</td>
</tr>
</tbody>
</table>
To remove a named standard ACL, use the `no ip access-list standard name` global configuration command.

Beginning in privileged EXEC mode, follow these steps to create an extended ACL using names:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3 deny {source [source-wildcard]</td>
<td>host source</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show access-lists [number</td>
<td>name]</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove a named extended ACL, use the `no ip access-list extended name` global configuration command.

When you are creating standard 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. This example shows how you can delete individual ACEs from the named access list `border-list`:

```bash
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

Being able to selectively remove lines from a named ACL is one reason you might use named ACLs instead of numbered ACLs.

After creating a named ACL, you can apply it to interfaces (see the “Applying an IPv4 ACL to an Interface” section on page 33-19) or to VLANs (see the “Configuring VLAN Maps” section on page 33-29).

### Using Time Ranges with 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 in the previous sections, the “Creating Standard and Extended IPv4 ACLs” section on page 33-7, and the “Creating Named Standard and Extended ACLs” section on page 33-14.

These are some of the many possible 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 TCAM. For this reason, you should be careful not to have several access lists configured to take effect in close succession (within a small number of minutes of each other.)

---

**Note**

The time range relies on the switch system clock; therefore, you need a reliable clock source. We recommend that you use Network Time Protocol (NTP) to synchronize the switch clock. For more information, see the “Managing the System Time and Date” section on page 6-1.
Beginning in privileged EXEC mode, follow these steps to configure a time-range parameter for an ACL:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>time-range time-range-name</td>
<td>Assign a meaningful name (for example, workhours) to the time range to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be created, and enter time-range configuration mode. The name cannot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>contain a space or quotation mark and must begin with a letter.</td>
</tr>
<tr>
<td>3</td>
<td>absolute [start time date]</td>
<td>Specify when the function it will be applied to is operational.</td>
</tr>
<tr>
<td></td>
<td>[end time date]</td>
<td>• You can use only one absolute statement in the time range. If you</td>
</tr>
<tr>
<td></td>
<td>or periodic day-of-the-week hh:mm to</td>
<td>configure more than one absolute statement, only the one configured</td>
</tr>
<tr>
<td></td>
<td>[day-of-the-week] hh:mm</td>
<td>last is executed.</td>
</tr>
<tr>
<td></td>
<td>or periodic {weekdays</td>
<td>weekend</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configure different hours for weekdays and weekends.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show time-range</td>
<td>Verify the time-range configuration.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Repeat the steps if you have multiple items that you want in effect at different times.

To remove a configured time-range limitation, use the no time-range time-range-name global configuration command.

This example shows how to configure time ranges for workhours and to configure January 1, 2006, as a company holiday and to verify your configuration.

```bash
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
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.

```bash
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.

```console
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
  10 permit ip any any
Extended IP access list deny_access
  10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
  10 permit tcp any any time-range workhours (inactive)
```

### 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.

In this example, the workstation that belongs to Jones is allowed access, and the workstation that belongs to Smith is not allowed access:

```console
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 through
Switch(config)# access-list 1 deny 171.69.3.13
```

For an entry in a named IP ACL, use the `remark` access-list configuration command. To remove the remark, use the `no` form of this command.

In this example, the Jones subnet is not allowed to use outbound Telnet:

```console
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 host 171.69.2.88 any eq telnet
```
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.

For procedures for applying ACLs to interfaces, see the “Applying an IPv4 ACL to an Interface” section on page 33-19. For applying ACLs to VLANs, see the “Configuring VLAN Maps” section on page 33-29.

Beginning in privileged EXEC mode, follow these steps to restrict incoming and outgoing connections between a virtual terminal line and the addresses in an ACL:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 line [console</td>
<td>vty] line-number</td>
</tr>
<tr>
<td></td>
<td>• console—Specify the console terminal line. The console port is DCE.</td>
</tr>
<tr>
<td></td>
<td>• vty—Specify a virtual terminal for remote console access.</td>
</tr>
<tr>
<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 3 access-class access-list-number {in</td>
<td>out}</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Display the access list configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove an ACL from a terminal line, use the no access-class access-list-number {in | out} line configuration command.

Applying an IPv4 ACL to an Interface

Note these guidelines:

• Apply an ACL only to inbound Layer 2 ports.
• Apply an ACL to either outbound or inbound Layer 3 interfaces.
• When controlling access to an interface, you can use a named or numbered ACL.
• If you apply an ACL to a port that is a member of a VLAN, the port ACL takes precedence over an ACL applied to the VLAN interface.
• If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over an input Layer 3 ACL applied to the VLAN interface or a VLAN map applied to the VLAN. The port ACL always filters incoming packets received on the Layer 2 port.
• If you apply an ACL to a Layer 3 interface and routing is not enabled, the ACL only filters packets that are intended for the CPU, such as SNMP, Telnet, or web traffic. You do not have to enable routing to apply ACLs to Layer 2 interfaces.
• When private VLANs are configured, you can apply router ACLs only on the primary-VLAN SVIs. The ACL is applied to both primary and secondary VLAN Layer 3 traffic.
Beginning in privileged EXEC mode, follow these steps to control access to an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Identify a specific interface for configuration, and enter interface configuration mode. The interface can be a Layer 2 interface (port ACL), or a Layer 3 interface (router ACL).</td>
</tr>
<tr>
<td>Step 3 ip access-group {access-list-number</td>
<td>Control access to the specified interface. The out keyword is not supported for Layer 2 interfaces (port ACLs).</td>
</tr>
<tr>
<td>name</td>
<td>in</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Display the access list configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the specified access group, use the no ip access-group {access-list-number | name} {in | out} interface configuration command.

This example shows how to apply access list 2 to a port to filter packets entering the port:

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in

When you apply the ip access-group interface configuration command to a Layer 3 interface (an SVI, a Layer 3 EtherChannel, or a routed port), the interface must have been configured with an IP address. Layer 3 access groups filter packets that are routed or are received by Layer 3 processes on the CPU. They do not affect packets bridged within a VLAN.

For inbound ACLs, after receiving a packet, the switch checks the packet against the ACL. If the ACL permits the packet, the switch continues to process the packet. If the ACL rejects the packet, the switch discards the packet.

For outbound ACLs, after receiving and sending 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.

By default, the input interface sends ICMP Unreachable messages whenever a packet is discarded, regardless of whether the packet was discarded because of an ACL on the input interface or because of an ACL on the output interface. ICMP Unreachables are normally limited to no more than one every one-half second per input interface, but this can be changed by using the ip icmp rate-limit unreachable global configuration command.

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.
Hardware and Software Treatment of IP ACLs

ACL processing is primarily accomplished in hardware, but requires forwarding of some traffic flows to the CPU for software processing. If the hardware reaches its capacity to store ACL configurations, packets are sent to the CPU for forwarding. The forwarding rate for software-forwarded traffic is substantially less than for hardware-forwarded traffic.

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 (forwarded in software). Software forwarding of packets might adversely impact the performance of the switch, depending on the number of CPU cycles that this consumes.

For router ACLs, other factors can cause packets to be sent to the CPU:

- Using the log keyword
- Generating ICMP unreachable messages

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.

If router ACL configuration cannot be applied in hardware, packets arriving in a VLAN that must be routed are routed in software, but are bridged in hardware. If ACLs cause large numbers of packets to be sent to the CPU, the switch performance can be negatively affected.

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. Use the show access-lists hardware counters privileged EXEC command to obtain some basic hardware ACL statistics for switched and routed packets.

Troubleshooting ACLs

If this ACL manager message appears and [chars] is the access-list name,

ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]

The switch has insufficient resources to create a hardware representation of the ACL. The resources include hardware memory and label space but not CPU memory. A lack of available logical operation units or specialized hardware resources causes this problem. Logical operation units are needed for a TCP flag match or a test other than eq (ne, gt, lt, or range) on TCP, UDP, or SCTP port numbers.

Use one of these workarounds:

- Modify the ACL configuration to use fewer resources.
- Rename the ACL with a name or number that alphanumerically precedes the ACL names or numbers.

To determine the specialized hardware resources, enter the show platform layer4 acl map privileged EXEC command. If the switch does not have available resources, the output shows that index 0 to index 15 are not available.

For more information about configuring ACLs with insufficient resources, see CSCsq63926 in the Bug Toolkit.
For example, if you apply this ACL to an interface:

```
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
```

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 alphabetically 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 TCAM.

Router 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 a router 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 and routed in hardware.

IPv4 ACL Configuration Examples

This section provides examples of configuring and applying IPv4 ACLs. For detailed information about compiling ACLs, see the Cisco IOS Security Configuration Guide, Release 12.2 and to the Configuring IP Services” section in the “IP Addressing and Services” chapter of the Cisco IOS IP Configuration Guide, Release 12.2.

Figure 33-3 shows a small networked office environment with routed Port 2 connected to Server A, containing benefits and other information that all employees can access, and routed Port 1 connected to Server B, containing confidential payroll data. All users can access Server A, but Server B has restricted access.

Use router ACLs to do this in one of two ways:

- Create a standard ACL, and filter traffic coming to the server from Port 1.
- Create an extended ACL, and filter traffic coming from the server into Port 1.
Chapter 33 Configuring Network Security with ACLs

Configuring IPv4 ACLs

This example uses a standard ACL to filter traffic coming into Server B from a port, permitting traffic only from Accounting’s source addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic coming out of routed Port 1 from the specified source address.

Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch(config)# show access-lists
Standard IP access list 6
  permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 6 out

This example uses an extended ACL to filter traffic coming from Server B into a port, permitting traffic from any source address (in this case Server B) to only the Accounting destination addresses 172.20.128.64 to 172.20.128.95. The ACL is applied to traffic going into routed Port 1, permitting it to go only to the specified destination addresses. Note that with extended ACLs, you must enter the protocol (IP) before the source and destination information.

Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch(config)# show access-lists
Extended IP access list 106
  permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 106 in

Figure 33-3 Using Router ACLs to Control Traffic

Server A
Benefits

Server B
Payroll

Port 2
Port 1

Accounting
172.20.128.64-95

Human Resources
172.20.128.0-31

101354
Numbered ACLs

In this example, network 36.0.0.0 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 36.0.0.0 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 36.0.0.0 subnets. The ACL is applied to packets entering a port.

Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in

Extended ACLs

In this example, the first line permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 128.88.1.2. The third line permits incoming ICMP messages for error feedback.

Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in

In this example, suppose that you have a network connected to the Internet, and you want any host on the network to be able to form TCP connections to any host on the Internet. However, you do not want IP hosts to be able to form TCP connections to hosts on your network, except to the mail (SMTP) port of a dedicated mail host.

SMTP uses TCP port 25 on one end of the connection and a random port number on the other end. The same port numbers are used throughout the life of the connection. Mail packets coming in from the Internet have a destination port of 25. Outbound packets have the port numbers reversed. Because the secure system of the network always accepts mail connections on port 25, the incoming and outgoing services are separately controlled. The ACL must be configured as an input ACL on the outbound interface and an output ACL on the inbound interface.

In this example, the network is a Class B network with the address 128.88.0.0, and the mail host address is 128.88.1.2. The established keyword is used only for the TCP to show an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which show that the packet belongs to an existing connection. Gigabit Ethernet interface 1 is the interface that connects the router to the Internet.

Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in

Named 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

The Internet_filter ACL is applied to outgoing traffic and the marketing_group ACL is applied to incoming traffic on a Layer 3 port.

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in

### 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 gigabitethernet0/2
Switch(config-if)# ip access-group strict in

### 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-standard-nacl)# remark Do not allow Jones subnet through
Switch(config-standard-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
```

### ACL Logging

Two variations of logging are supported on router ACLs. The `log` keyword sends an informational logging message to the console about the packet that matches the entry; the `log-input` keyword includes the input interface in the log entry.

In this example, standard named access list `stan1` denies traffic from 10.1.1.0 0.0.0.255, allows traffic from all other sources, and includes the `log` keyword.

```
Switch(config)# ip access-list standard stan1
Switch(config-standard-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-standard-nacl)# permit any log
Switch(config-standard-nacl)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
   Console logging: level debugging, 37 messages logged
   Monitor logging: level debugging, 0 messages logged
   Buffer logging: level debugging, 37 messages logged
   File logging: disabled
   Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):
00:00:48: NTP: authentication delay calculation problems
(output truncated)
```

```
00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

In this example, a named extended access list `ext1` that permits ICMP packets from any source to 10.1.1.0 0.0.0.255 and denies all UDP packets.

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip access-group ext1 in
```
Creating Named MAC Extended ACLs

You can filter non-IPv4 traffic on a VLAN or on a Layer 2 interface by using MAC addresses and named MAC extended ACLs. The procedure is similar to that of configuring other extended named ACLs.

**Note**

You cannot apply named MAC extended ACLs to Layer 3 interfaces.

For more information about the supported non-IP protocols in the `mac access-list extended` command, see the command reference for this release.

**Note**

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.

Beginning in privileged EXEC mode, follow these steps to create a named MAC extended ACL:

<table>
<thead>
<tr>
<th>Command</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>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>mac access-list extended name</code></td>
<td>Define an extended MAC access list using a name.</td>
</tr>
</tbody>
</table>
Creating Named MAC Extended ACLs

Use the `no mac access-list extended name` global configuration command to delete the entire ACL. You can also delete individual ACEs from named MAC extended ACLs.

This example shows how to create and display an access list named `mac1`, denying only EtherType DECnet Phase IV traffic, but permitting all other types of traffic.

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch# show access-lists
Extended MAC access list mac1
  10 deny   any any decnet-iv
  20 permit any any
```

Applying a MAC ACL to 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:

- If you apply an ACL to a Layer 2 interface that is a member of a VLAN, the Layer 2 (port) ACL takes precedence over an input Layer 3 ACL applied to the VLAN interface or a VLAN map applied to the VLAN. Incoming packets received on the Layer 2 port are always filtered by the port ACL.
- 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.
Chapter 33      Configuring Network Security with ACLs

Configuring VLAN Maps

To remove the specified access group, use the no mac access-group {name} command.

This example shows how to apply MAC access list mac1 to a port to filter packets entering the port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mac access-group mac1 in
```

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.

After receiving a packet, the switch checks it against the inbound ACL. If the ACL permits it, the switch continues to process the packet. If the ACL rejects the packet, the switch discards it. When you apply an undefined ACL to an interface, the switch acts as if the ACL has not been applied and permits all packets. Remember this behavior if you use undefined ACLs for network security.

### Configuring VLAN Maps

This section describes how to configure VLAN maps, which is the only way to control filtering within a VLAN. VLAN maps have no direction. To filter traffic in a specific direction by using a VLAN map, you need to include an ACL with specific source or destination addresses. If there is a match clause for that type of packet (IP or MAC) in the VLAN map, the default action is to drop the packet if the packet does not match any of the entries within the map. If there is no match clause for that type of packet, the default is to forward the packet.

For complete syntax and usage information for the commands used in this section, see the command reference for this release.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>mac access-group {name} {in}</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mac access-group [interface interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
To create a VLAN map and apply it to one or more VLANs, perform these steps:

**Step 1** Create the standard or extended IPv4 ACLs or named MAC extended ACLs that you want to apply to the VLAN. See the “Creating Standard and Extended IPv4 ACLs” section on page 33-7 and the “Creating a VLAN Map” section on page 33-31.

**Step 2** Enter the `vlan access-map` global configuration command to create a VLAN ACL map entry.

**Step 3** In access-map configuration mode, optionally enter an **action**—**forward** (the default) or **drop**—and enter the **match** command to specify an IP packet or a non-IP packet (with only a known MAC address) and to match the packet against one or more ACLs (standard or extended).

**Note** If the VLAN map is configured with a match clause for a type of packet (IP or MAC) and the map action is drop, all packets that match the type are dropped. If the VLAN map has no match clause, and the configured action is drop, all IP and Layer 2 packets are dropped.

**Step 4** Use the `vlan filter` global configuration command to apply a VLAN map to one or more VLANs.

These sections contain this configuration information:

- VLAN Map Configuration Guidelines, page 33-30
- Creating a VLAN Map, page 33-31
- Applying a VLAN Map to a VLAN, page 33-34
- Using VLAN Maps in Your Network, page 33-34

**VLAN Map Configuration Guidelines**

Follow these guidelines when configuring VLAN maps:

- If there is no ACL configured to deny traffic on an interface and no VLAN map is configured, all traffic is permitted.
- Each VLAN map consists of a series of entries. The order of entries in an VLAN map is important. A packet that comes into the switch is tested against the first entry in the VLAN map. If it matches, the action specified for that part of the VLAN map is taken. If there is no match, the packet is tested against the next entry in the map.
- If the VLAN map has at least one match clause for the type of packet (IP or MAC) and the packet does not match any of these match clauses, the default is to drop the packet. If there is no match clause for that type of packet in the VLAN map, the default is to forward the packet.
- The system might take longer to boot up if you have configured a very large number of ACLs.
- Logging is not supported for VLAN maps.
- When a switch has an IP access list or MAC access list applied to a Layer 2 interface, and you apply a VLAN map to a VLAN that the port belongs to, the port ACL takes precedence over the VLAN map.
- If VLAN map configuration cannot be applied in hardware, all packets in that VLAN must be bridged and routed by software.
- You can configure VLAN maps on primary and secondary VLANs. However, we recommend that you configure the same VLAN maps on private-VLAN primary and secondary VLANs.
When a frame is Layer-2 forwarded within a private VLAN, the same VLAN map is applied at the ingress side and at the egress side. When a frame is routed from inside a private VLAN to an external port, the private-VLAN map is applied at the ingress side.

- For frames going upstream from a host port to a promiscuous port, the VLAN map configured on the secondary VLAN is applied.
- For frames going downstream from a promiscuous port to a host port, the VLAN map configured on the primary VLAN is applied.

To filter out specific IP traffic for a private VLAN, you should apply the VLAN map to both the primary and secondary VLANs. For more information about private VLANs, see Chapter 15, “Configuring Private VLANs.”

For configuration examples, see the “Using VLAN Maps in Your Network” section on page 33-34.

For information about using both router ACLs and VLAN maps, see the “VLAN Maps and Router ACL Configuration Guidelines” section on page 33-37.

### Creating a VLAN Map

Each VLAN map consists of an ordered series of entries. Beginning in privileged EXEC mode, follow these steps to create, add to, or delete a VLAN map entry:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>vlan access-map name [number]</td>
<td>Create a VLAN map, and give it a name and (optionally) a number. The number is the sequence number of the entry within the map. When you create VLAN maps with the same name, numbers are assigned sequentially in increments of 10. When modifying or deleting maps, you can enter the number of the map entry that you want to modify or delete. Entering this command changes to access-map configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>action {drop</td>
<td>forward}</td>
</tr>
<tr>
<td>4</td>
<td>match {ip</td>
<td>mac} address {name</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>6</td>
<td>show running-config</td>
<td>Display the access list configuration.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no vlan access-map name global configuration command to delete a map. Use the no vlan access-map name number global configuration command to delete a single sequence entry from within the map.

Use the no action access-map configuration command to enforce the default action, which is to forward. VLAN maps do not use the specific permit or deny keywords. To deny a packet by using VLAN maps, create an ACL that would match the packet, and set the action to drop. A permit in the ACL counts as a match. A deny in the ACL means no match.
Examples of ACLs and VLAN Maps

These examples show how to create ACLs and VLAN maps that for specific purposes.

Example 1

This example shows how to create an ACL and a VLAN map to deny a packet. In the first map, any packets that match the ip1 ACL (TCP packets) would be dropped. You first create the ip1 ACL to permit any TCP packet and no other packets. Because there is a match clause for IP packets in the VLAN map, the default action is to drop any IP packet that does not match any of the match clauses.

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

This example shows how to create a VLAN map to permit a packet. ACL ip2 permits UDP packets and any packets that match the ip2 ACL are forwarded. In this map, any IP packets that did not match any of the previous ACLs (that is, packets that are not TCP packets or UDP packets) would get dropped.

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

Example 2

In this example, the VLAN map has a default action of drop for IP packets and a default action of forward for MAC packets. Used with standard ACL 101 and extended named access lists igmp-match and tcp-match, the map will have the following results:

- Forward all UDP packets
- Drop all IGMP packets
- Forward all TCP packets
- Drop all other IP packets
- Forward all non-IP packets

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```
Example 3

In this example, the VLAN map has a default action of drop for MAC packets and a default action of forward for IP packets. Used with MAC extended access lists good-hosts and good-protocols, the map will have the following results:

- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Forward MAC packets with decnet-iv or vines-ip protocols
- Drop all other non-IP packets
- Forward all IP packets

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any decnet-ip
Switch(config-ext-macl)# permit any any vines-ip
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

Example 4

In this example, the VLAN map has a default action of drop for all packets (IP and non-IP). Used with access lists tcp-match and good-hosts from Examples 2 and 3, the map will have the following results:

- Forward all TCP packets
- Forward MAC packets from hosts 0000.0c00.0111 and 0000.0c00.0211
- Drop all other IP packets
- Drop all other MAC packets

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```
Applying a VLAN Map to a VLAN

Beginning in privileged EXEC mode, follow these steps to apply a VLAN map to one or more VLANs:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>vlan filter mapname vlan-list list</td>
</tr>
<tr>
<td>Step 3</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 4</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the VLAN map, use the `no vlan filter mapname vlan-list list` global configuration command.

This example shows how to apply VLAN map 1 to VLANs 20 through 22:

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

Using VLAN Maps in Your Network

These sections describes some typical uses for VLAN maps:

- Wiring Closet Configuration, page 33-34
- Denying Access to a Server on Another VLAN, page 33-35

Wiring Closet Configuration

In a wiring closet configuration, routing might not be enabled on the switch. In this configuration, the switch can still support a VLAN map and a QoS classification ACL. In Figure 33-4, assume that Host X and Host Y are in different VLANs and are connected to wiring closet switches A and C. Traffic from Host X to Host Y is eventually being routed by Switch B, a Layer 3 switch with routing enabled. Traffic from Host X to Host Y can be access-controlled at the traffic entry point, Switch A.
Chapter 33 Configuring Network Security with ACLs

Configuring VLAN Maps

Figure 33-4 Wiring Closet Configuration

If you do not want HTTP traffic switched from Host X to Host Y, you can configure a VLAN map on Switch A to drop all HTTP traffic from Host X (IP address 10.1.1.32) to Host Y (IP address 10.1.1.34) at Switch A and not bridge it to Switch B.

First, define the IP access list http that permits (matches) any TCP traffic on the HTTP port.

```config
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

Next, create VLAN access map map2 so that traffic that matches the http access list is dropped and all other IP traffic is forwarded.

```config
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

Then, apply VLAN access map map2 to VLAN 1.

```config
Switch(config)# vlan filter map2 vlan 1
```

Denying Access to a Server on Another VLAN

You can restrict access to a server on another VLAN. For example, server 10.1.1.100 in VLAN 10 needs to have access denied to these hosts (see Figure 33-5):

- Hosts in subnet 10.1.2.0/8 in VLAN 20 should not have access.
- Hosts 10.1.1.4 and 10.1.1.8 in VLAN 10 should not have access.
This example shows how to deny access to a server on another VLAN by creating the VLAN map SERVER1 that denies access to hosts in subnet 10.1.2.0/8, host 10.1.1.4, and host 10.1.1.8 and permits other IP traffic. The final step is to apply the map SERVER1 to VLAN 10.

**Step 1** Define the IP ACL that will match the correct packets.

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit
```

**Step 2** Define a VLAN map using this ACL that will drop IP packets that match SERVER1_ACL and forward IP packets that do not match the ACL.

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

**Step 3** Apply the VLAN map to VLAN 10.

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

---

**Using VLAN Maps with Router ACLs**

To access control both bridged and routed traffic, you can use VLAN maps only or a combination of router ACLs and VLAN maps. You can define router ACLs on both input and output routed VLAN interfaces, and you can define a VLAN map to access control the bridged traffic.

If a packet flow matches a VLAN-map deny clause in the ACL, regardless of the router ACL configuration, the packet flow is denied.
Chapter 33 Configuring Network Security with ACLs

Using VLAN Maps with Router ACLs

Note

When you use router ACLs with VLAN maps, packets that require logging on the router ACLs are not logged if they are denied by a VLAN map.

If the VLAN map has a match clause for the type of packet (IP or MAC) and the packet does not match the type, the default is to drop the packet. If there is no match clause in the VLAN map, and no action specified, the packet is forwarded if it does not match any VLAN map entry.

These sections contain information about using VLAN maps with router ACLs:

- VLAN Maps and Router ACL Configuration Guidelines, page 33-37
- Examples of Router ACLs and VLAN Maps Applied to VLANs, page 33-38

VLAN Maps and Router ACL Configuration Guidelines

These guidelines are for configurations where you need to have an router ACL and a VLAN map on the same VLAN. These guidelines do not apply to configurations where you are mapping router ACLs and VLAN maps on different VLANs.

The switch hardware provides one lookup for security ACLs for each direction (input and output); therefore, you must merge a router ACL and a VLAN map when they are configured on the same VLAN. Merging the router ACL with the VLAN map might significantly increase the number of ACEs.

If you must configure a router ACL and a VLAN map on the same VLAN, use these guidelines for both router ACL and VLAN map configuration:

- You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.
- Whenever possible, try to write the ACL with all entries having a single action except for the final, default action of the other type. That is, write the ACL using one of these two forms:
  
  ```
  permit...
  permit...
  permit...
  deny ip any any
  ```
  
  or
  
  ```
  deny...
  deny...
  deny...
  permit ip any any
  ```
- To define multiple actions in an ACL (permit, deny), group each action type together to reduce the number of entries.
- Avoid including Layer 4 information in an ACL; adding this information complicates the merging process. The best merge results are obtained if the ACLs are filtered based on IP addresses (source and destination) and not on the full flow (source IP address, destination IP address, protocol, and protocol ports). It is also helpful to use don’t care bits in the IP address, whenever possible.

If you need to specify the full-flow mode and the ACL contains both IP ACEs and TCP/UDP/ICMP ACEs with Layer 4 information, put the Layer 4 ACEs at the end of the list. This gives priority to the filtering of traffic based on IP addresses.
Examples of Router ACLs and VLAN Maps Applied to VLANs

This section gives examples of applying router ACLs and VLAN maps to a VLAN for switched, bridged, routed, and multicast packets. Although the following illustrations show packets being forwarded to their destination, each time the packet’s path crosses a line indicating a VLAN map or an ACL, it is also possible that the packet might be dropped, rather than forwarded.

ACLs and Switched Packets

Figure 33-6 shows how an ACL is applied on packets that are switched within a VLAN. Packets switched within the VLAN without being routed or forwarded by fallback bridging are only subject to the VLAN map of the input VLAN.

Figure 33-6 Applying ACLs on Switched Packets

ACLs and Bridged Packets

Figure 33-7 shows how an ACL is applied on fallback-bridged packets. For bridged packets, only Layer 2 ACLs are applied to the input VLAN. Only non-IP, non-ARP packets can be fallback-bridged.
**ACLs and Routed Packets**

Figure 33-8 shows how ACLs are applied on routed packets. For routed packets, the ACLs are applied in this order:

1. VLAN map for input VLAN
2. Input router ACL
3. Output router ACL
4. VLAN map for output VLAN

**Figure 33-8 Applying ACLs on Routed Packets**
ACLs and Multicast Packets

Figure 33-9 shows how ACLs are applied on packets that are replicated for IP multicasting. A multicast packet being routed has two different kinds of filters applied: one for destinations that are other ports in the input VLAN and another for each of the destinations that are in other VLANs to which the packet has been routed. The packet might be routed to more than one output VLAN, in which case a different router output ACL and VLAN map would apply for each destination VLAN.

The final result is that the packet might be permitted in some of the output VLANs and not in others. A copy of the packet is forwarded to those destinations where it is permitted. However, if the input VLAN map (VLAN 10 map in Figure 33-9) drops the packet, no destination receives a copy of the packet.
Displaying IPv4 ACL Configuration

You can display the ACLs that are configured on the switch, and you can display the ACLs that have been applied to interfaces and VLANs.

When you use the `ip access-group` interface configuration command to apply ACLs to a Layer 2 or 3 interface, you can display the access groups on the interface. You can also display the MAC ACLs applied to a Layer 2 interface. You can use the privileged EXEC commands as described in Table 33-2 to display this information.

<table>
<thead>
<tr>
<th>Table 33-2 Commands for Displaying Access Lists and Access Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>show access-lists [number</td>
</tr>
<tr>
<td>show ip access-lists [number</td>
</tr>
<tr>
<td>show ip interface interface-id</td>
</tr>
<tr>
<td>show running-config [interface interface-id]</td>
</tr>
<tr>
<td>show mac access-group [interface interface-id]</td>
</tr>
</tbody>
</table>

You can also display information about VLAN access maps or VLAN filters. Use the privileged EXEC commands in Table 33-3 to display VLAN map information.

<table>
<thead>
<tr>
<th>Table 33-3 Commands for Displaying VLAN Map Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>show vlan access-map [mapname]</td>
</tr>
<tr>
<td>show vlan filter [access-map name</td>
</tr>
</tbody>
</table>
Configuring QoS

This chapter describes how to configure quality of service (QoS) by using automatic QoS (auto-QoS) commands or by using standard QoS commands on the Catalyst 3560 switch. With QoS, you can provide preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

You can configure QoS on physical ports and on switch virtual interfaces (SVIs). Other than to apply policy maps, you configure the QoS settings, such as classification, queueing, and scheduling, the same way on physical ports and SVIs. When configuring QoS on a physical port, you apply a nonhierarchical policy map to a port. When configuring QoS on an SVI, you apply a nonhierarchical or a hierarchical policy map. In the Catalyst 3750 Metro switch documentation, nonhierarchical policy maps are referred to as nonhierarchical single-level policy maps, and hierarchical policy maps are referred to as hierarchical dual-level policy maps.

Note
For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

This chapter consists of these sections:

- Understanding QoS, page 34-2
- Configuring Auto-QoS, page 34-21
- Displaying Auto-QoS Information, page 34-34
- Configuring Standard QoS, page 34-34
- Displaying Standard QoS Information, page 34-84

The switch supports some of the modular QoS CLI (MQC) commands. For more information about the MQC commands, see the “Modular Quality of Service Command-Line Interface Overview”: http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmcli2.html
Understanding QoS

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, an emerging standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification can also be carried in the Layer 2 frame. These special bits in the Layer 2 frame or a Layer 3 packet are described here and shown in Figure 34-1:

- Prioritization bits in Layer 2 frames:
  - Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On ports configured as Layer 2 ISL trunks, all traffic is in ISL frames.
  - Layer 2 IEEE 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 IEEE 802.1Q trunks, all traffic is in IEEE 802.1Q frames except for traffic in the native VLAN.
  - Other frame types cannot carry Layer 2 CoS values.
  - Layer 2 CoS values range from 0 for low priority to 7 for high priority.

- Prioritization bits in Layer 3 packets:
  - Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.
  - IP precedence values range from 0 to 7.
  - DSCP values range from 0 to 63.

Note
Cisco IOS Release 12.2(52)SE and later supports IPv6 port-based trust with the dual IPv4 and IPv6 Switch Database Management (SDM) templates. You must reload the switch with the dual IPv4 and IPv6 templates for switches running IPv6. For more information, see Chapter 7, “Configuring SDM Templates.”
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 happen 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 DiffServ 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 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.
Basic QoS Model

To implement QoS, the switch must distinguish packets or flow 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 34-2 shows the basic QoS model. Actions at the ingress port include classifying traffic, policing, marking, queueing, and scheduling:

- Classifying a distinct path for a packet by associating it with a QoS label. The switch maps the CoS or DSCP in the packet to a QoS label to distinguish one kind of traffic from another. The QoS label that is generated identifies all future QoS actions to be performed on this packet. For more information, see the “Classification” section on page 34-5.

- 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. For more information, see the “Policing and Marking” section on page 34-9.

- 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, mark down the QoS label in the packet, or drop the packet). For more information, see the “Policing and Marking” section on page 34-9.

- Queueing evaluates the QoS label and the corresponding DSCP or CoS value to select into which of the two ingress queues to place a packet. Queueing is enhanced with the weighted tail-drop (WTD) algorithm, a congestion-avoidance mechanism. If the threshold is exceeded, the packet is dropped. For more information, see the “Queueing and Scheduling Overview” section on page 34-14.

- Scheduling services the queues based on their configured shaped round robin (SRR) weights. One of the ingress queues is the priority queue, and SRR services it for its configured share before servicing the other queue. For more information, see the “SRR Shaping and Sharing” section on page 34-15.

Actions at the egress port include queueing and scheduling:

- Queueing evaluates the QoS packet label and the corresponding DSCP or CoS value before selecting which of the four egress queues to use. Because congestion can occur when multiple ingress ports simultaneously send data to an egress port, WTD differentiates traffic classes and subjects the packets to different thresholds based on the QoS label. If the threshold is exceeded, the packet is dropped. For more information, see the “Queueing and Scheduling Overview” section on page 34-14.

- Scheduling services the four egress queues based on their configured SRR shared or shaped weights. One of the queues (queue 1) can be the expedited queue, which is serviced until empty before the other queues are serviced.
Classification

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 queueing and scheduling actions to perform on the packet. The label is mapped according to the trust setting and the packet type as shown in Figure 34-3 on page 34-7.

You specify which fields in the frame or packet that you want to use to classify incoming traffic. For non-IP traffic, you have these classification options as shown in Figure 34-3:

- Trust the CoS value in the incoming frame (configure the port to trust CoS). 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 IEEE 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.

- Trust the DSCP or trust IP precedence 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.

- 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.
For IP traffic, you have these classification options as shown in Figure 34-3:

- 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.

- 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.

- Trust the IP precedence value in the incoming packet (configure the port to trust IP precedence), and generate a DSCP value for the packet by using the configurable IP-precedence-to-DSCP map. The IP Version 4 specification defines the 3 most-significant bits of the 1-byte ToS field as the IP precedence. IP precedence values range from 0 for low priority to 7 for high priority.

- 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.

- 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.

For information on the maps described in this section, see the “Mapping Tables” section on page 34-13. For configuration information on port trust states, see the “Configuring Classification Using Port Trust States” section on page 34-41.

After classification, the packet is sent to the policing, marking, and the ingress queueing and scheduling stages.
Figure 34-3  Classification Flowchart

Start

Read ingress interface configuration for classification.

IP and non-IP traffic

Trust CoS (IP and non-IP traffic).

Trust DSCP (IP traffic).

Trust IP precedence (non-IP traffic).

Generate DSCP from CoS-to-DSCP map. Use the DSCP value to generate the QoS label.

Done

Are there any (more) QoS ACLs configured for this interface?

No

Yes

Check if packet came with CoS label (tag).

Use CoS from frame.

Assign default port CoS.

Assign the DSCP or CoS as specified by ACL action to generate the QoS label.

Assign the default DSCP (0).

Generate the DSCP by using the CoS-to-DSCP map.

Done

Generate the DSCP based on IP precedence in packet. Use the IP-precedence-to-DSCP map. Use the DSCP value to generate the QoS label.

Done

(Optional) Modify the DSCP by using the DSCP-to-DSCP-mutation map. Use the DSCP value to generate the QoS label.

Yes

No

Check if packet came with CoS label (tag).

Use the CoS value to generate the QoS label.

Assign the default port CoS and generate a DSCP from the CoS-to-DSCP map.

Generate the DSCP by using the CoS-to-DSCP map.

Done

Read next ACL. Is there a match with a "permit" action?

No

Yes

Assign DSCP identical to DSCP in packet.

Assign the default DSCP (0).

Trust CoS (IP and non-IP traffic).

Trust DSCP (IP traffic).

Trust IP precedence (IP traffic).

Generate DSCP from CoS-to-DSCP map. Use the DSCP value to generate the QoS label.

Done

Generate the DSCP based on IP precedence in packet. Use the IP-precedence-to-DSCP map. Use the DSCP value to generate the QoS label.

Done

(Optional) Modify the DSCP by using the DSCP-to-DSCP-mutation map. Use the DSCP value to generate the QoS label.

Yes

No

Check if packet came with CoS label (tag).

Use CoS from frame.

Assign default port CoS.

Assign the DSCP or CoS as specified by ACL action to generate the QoS label.

Assign the default DSCP (0).

Generate the DSCP by using the CoS-to-DSCP map.

Done

Are there any (more) QoS ACLs configured for this interface?

No

Yes

Read next ACL. Is there a match with a "permit" action?

No

Yes

Assign DSCP identical to DSCP in packet.

Assign the default DSCP (0).

Generate the DSCP based on IP precedence in packet. Use the IP-precedence-to-DSCP map. Use the DSCP value to generate the QoS label.

Done

(Optional) Modify the DSCP by using the DSCP-to-DSCP-mutation map. Use the DSCP value to generate the QoS label.

Yes

No

Check if packet came with CoS label (tag).

Use CoS from frame.

Assign default port CoS.

Assign the DSCP or CoS as specified by ACL action to generate the QoS label.

Assign the default DSCP (0).

Generate the DSCP by using the CoS-to-DSCP map.
Classification Based on QoS ACLs

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (class). In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings than with 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.
- 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, 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.

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. For configuration information, see the “Configuring a QoS Policy” section on page 34-47.

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 or IP precedence 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, DSCP, or IP precedence values in the traffic class; setting a specific DSCP or IP precedence 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 that does not meet the match criteria specified in the traffic classes) 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`, `trust`, or `set` policy-map configuration and policy-map class configuration commands.

The policy map can contain the `police` and `police aggregate` 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.

You can apply a nonhierarchical policy map to a physical port or an SVI. However, a hierarchical policy map can only be applied to an SVI. A hierarchical policy map contains two levels. The first level, the VLAN level, specifies the actions to be taken against a traffic flow on the SVI. The second level, the interface level, specifies the actions to be taken against the traffic on the physical ports that belong to the SVI. The interface-level actions are specified in the interface-level policy map.

For more information, see the “Policing and Marking” section on page 34-9. For configuration information, see the “Configuring a QoS Policy” section on page 34-47.

**Policing and Marking**

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 as shown in Figure 34-4.

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. For information on the policed-DSCP map, see the “Mapping Tables” section on page 34-13. 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 (either individual or aggregate policers) on a physical port or an SVI. On a physical port, you can configure the trust state, set a new DSCP or IP precedence value in the packet, or define an individual or aggregate policer. For more information about configuring policing on physical ports, see the “Policing on Physical Ports” section on page 34-10. When configuring policy maps on an SVI, you can create a hierarchical policy map and can define an individual policer only in the secondary interface-level policy map. For more information, see the “Policing on SVIs” section on page 34-11.

After you configure the policy map and policing actions, attach the policy to an ingress port or SVI by using the `service-policy` interface configuration command. For configuration information, see the “Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps” section on page 34-53, the “Classifying, Policing, and Marking Traffic on SVIs by Using Hierarchical Policy Maps” section on page 34-57, and the “Classifying, Policing, and Marking Traffic by Using Aggregate Policers” section on page 34-64.
Policing on Physical Ports

In policy maps on physical ports, you can create these types of policers:

- Individual—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 `police` policy-map class configuration command.

- Aggregate—QoS applies the bandwidth limits specified in an aggregate policer cumulatively to all matched traffic flows. You configure this type of policer by specifying the aggregate policer name within a policy map by using the `police aggregate` policy-map class configuration command. You specify the bandwidth limits of the policer by using the `mls qos aggregate-policer` global configuration command. In this way, the aggregate policer is shared by multiple classes of traffic within a policy map.

> Note  You can configure only individual policers on an SVI.

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-b/s), 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 or the `mls qos aggregate-policer` global 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 or the `mls qos aggregate-policer` global configuration command.

**Figure 34-4** shows the policing and marking process. These types of policy maps are configured:

- A nonhierarchical policy map on a physical port.

- The interface level of a hierarchical policy map attached to an SVI. The physical ports are specified in this secondary policy map.
Policing on SVIs

**Note** Before configuring a hierarchical policy map with individual policers on an SVI, you must enable VLAN-based QoS on the physical ports that belong to the SVI. Though a policy map is attached to the SVI, the individual policers only affect traffic on the physical ports specified in the secondary interface level of the hierarchical policy map.

A hierarchical policy map has two levels. The first level, the VLAN level, specifies the actions to be taken against a traffic flow on an SVI. The second level, the interface level, specifies the actions to be taken against the traffic on the physical ports that belong to the SVI and are specified in the interface-level policy map.
When configuring policing on an SVI, you can create and configure a hierarchical policy map with these two levels:

- **VLAN level**—Create this primary level by configuring class maps and classes that specify the port trust state or set a new DSCP or IP precedence value in the packet. The VLAN-level policy map applies only to the VLAN in an SVI and does not support policers.

- **Interface level**—Create this secondary level by configuring class maps and classes that specify the individual policers on physical ports that belong to the SVI. The interface-level policy map only supports individual policers and does not support aggregate policers. You can configure different interface-level policy maps for each class defined in the VLAN-level policy map.

See the “Classifying, Policing, and Marking Traffic on SVIs by Using Hierarchical Policy Maps” section on page 34-57 for an example of a hierarchical policy map.

Figure 34-5 shows the policing and marking process when hierarchical policy maps on an SVI.

**Figure 34-5  Policing and Marking Flowchart on SVIs**

1. Start
2. Get the VLAN and interface-level classification results for the packet.
3. Is an interface-level policer configured for this packet?
   - No
   - Yes
5. Verify if the packet is in the profile by querying the policer.
   - No
   - Yes
6. Pass through
7. Verify the out-of-profile action configured for this policer.
   - Drop
8. Mark
9. Modify DSCP according to the policed-DSCP map. Generate a new QoS label.
10. Drop packet.
11. Done
Mapping Tables

During QoS processing, the switch represents the priority of all traffic (including non-IP traffic) with a QoS label based on the DSCP or CoS value from the classification stage:

- During classification, QoS uses configurable mapping tables to derive a corresponding DSCP or CoS value from a received CoS, DSCP, or IP precedence value. These maps include the CoS-to-DSCP map and the IP-precedence-to-DSCP map. You configure these maps by using the `mls qos map cos-dscp` and the `mls qos map ip-prec-dscp` global configuration commands.

  On an ingress port configured in the DSCP-trusted state, if the DSCP values are different between the QoS domains, you can apply the configurable DSCP-to-DSCP-mutation map to the port that is on the boundary between the two QoS domains. You configure this map by using the `mls qos map dscp-mutation` global configuration command.

- During policing, QoS can assign another DSCP value to an IP or a non-IP packet (if the packet is out of profile and the policer specifies a marked-down value). This configurable map is called the policed-DSCP map. You configure this map by using the `mls qos map policed-dscp` global configuration command.

- Before the traffic reaches the scheduling stage, QoS stores the packet in an ingress and an egress queue according to the QoS label. The QoS label is based on the DSCP or the CoS value in the packet and selects the queue through the DSCP input and output queue threshold maps or through the CoS input and output queue threshold maps. In addition to an ingress or an egress queue, the QoS label also identifies the WTD threshold value. You configure these maps by using the `mls qos srr-queue {input | output} dscp-map` and the `mls qos srr-queue {input | output} cos-map` global configuration commands.

The CoS-to-DSCP, DSCP-to-CoS, and the IP-precedence-to-DSCP maps have default values that might or might not be appropriate for your network.

The default DSCP-to-DSCP-mutation map and the default policed-DSCP map are null maps; they map an incoming DSCP value to the same DSCP value. The DSCP-to-DSCP-mutation map is the only map you apply to a specific port. All other maps apply to the entire switch.

For configuration information, see the “Configuring DSCP Maps” section on page 34-66.

For information about the DSCP and CoS input queue threshold maps, see the “Queueing and Scheduling on Ingress Queues” section on page 34-16. For information about the DSCP and CoS output queue threshold maps, see the “Queueing and Scheduling on Egress Queues” section on page 34-17.
Queueing and Scheduling Overview

The switch has queues at specific points to help prevent congestion as shown in Figure 34-6.

Figure 34-6  Ingress and Egress Queue Location

Because the total inbound bandwidth of all ports can exceed the bandwidth of the internal ring, ingress queues are located after the packet is classified, policed, and marked and before packets are forwarded into the switch fabric. Because multiple ingress ports can simultaneously send packets to an egress port and cause congestion, outbound queues are located after the internal ring.

Weighted Tail Drop

Both the ingress and 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 is 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 34-7 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 mean 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 this 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.
Understanding QoS

Figure 34-7  WTD and Queue Operation

For more information, see the “Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds” section on page 34-73, the “Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set” section on page 34-77, and the “Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID” section on page 34-80.

SRR Shaping and Sharing

Both the ingress and egress queues are serviced by SRR, which controls the rate at which packets are sent. On the ingress queues, SRR sends packets to the internal ring. On the egress queues, SRR sends packets to the egress port.

You can configure SRR on egress queues for sharing or for shaping. However, for ingress queues, sharing is the default mode, and it is the only mode supported.

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.

For more information, see the “Allocating Bandwidth Between the Ingress Queues” section on page 34-75, the “Configuring SRR Shaped Weights on Egress Queues” section on page 34-81, and the “Configuring SRR Shared Weights on Egress Queues” section on page 34-82.
Queueing and Scheduling on Ingress Queues

Figure 34-8 shows the queueing and scheduling flowchart for ingress ports.

![Figure 34-8 Queueing and Scheduling Flowchart for Ingress Ports](image)

Note: SRR services the priority queue for its configured share before servicing the other queue.

The switch supports two configurable ingress queues, which are serviced by SRR in shared mode only. Table 34-1 describes the queues.

<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>User traffic that is considered to be normal priority. You can configure three different thresholds to differentiate among the flows. You can use the <code>mls qos srr-queue input threshold</code>, the <code>mls qos srr-queue input dscp-map</code>, and the <code>mls qos srr-queue input cos-map</code> global configuration commands.</td>
</tr>
<tr>
<td>Expedite</td>
<td>High-priority user traffic such as differentiated services (DF) expedited forwarding or voice traffic. You can configure the bandwidth required for this traffic as a percentage of the total traffic by using the <code>mls qos srr-queue input priority-queue</code> global configuration command. The expedite queue has guaranteed bandwidth.</td>
</tr>
</tbody>
</table>

1. The switch uses two nonconfigurable queues for traffic that is essential for proper network operation.
You assign each packet that flows through the switch to a queue and to a threshold. Specifically, you map DSCP or CoS values to an ingress queue and map DSCP or CoS values to a threshold ID. You use the `mls qos srr-queue input dscp-map queue queue-id { dscp1...dscp8 | threshold threshold-id dscp1...dscp8}` or the `mls qos srr-queue input cos-map queue queue-id { cos1...cos8 | threshold threshold-id cos1...cos8}` global configuration command. You can display the DSCP input queue threshold map and the CoS input queue threshold map by using the `show mls qos maps` privileged EXEC command.

### WTD Thresholds

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 explicit WTD threshold percentages for threshold ID 1 and ID 2 to the ingress queues by using the `mls qos srr-queue input threshold queue-id threshold-percentage1 threshold-percentage2` global configuration command. Each threshold value is a percentage of the total number of allocated buffers for the queue. The drop threshold for threshold ID 3 is preset to the queue-full state, and you cannot modify it. For more information about how WTD works, see the “Weighted Tail Drop” section on page 34-14.

### Buffer and Bandwidth Allocation

You define the ratio (allocate the amount of space) with which to divide the ingress buffers between the two queues by using the `mls qos srr-queue input buffers percentage1 percentage2` global configuration command. The buffer allocation together with the bandwidth allocation control how much data can be buffered and sent before packets are dropped. You allocate bandwidth as a percentage by using the `mls qos srr-queue input bandwidth weight1 weight2` global configuration command. The ratio of the weights is the ratio of the frequency in which the SRR scheduler sends packets from each queue.

### Priority Queueing

You can configure one ingress queue as the priority queue by using the `mls qos srr-queue input priority-queue queue-id bandwidth weight` global configuration command. The priority queue should be used for traffic (such as voice) that requires guaranteed delivery because this queue is guaranteed part of the bandwidth regardless of the load on the internal ring.

SRR services the priority queue for its configured weight as specified by the `bandwidth` keyword in the `mls qos srr-queue input priority-queue queue-id bandwidth weight` global configuration command. Then, SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the `mls qos srr-queue input bandwidth weight1 weight2` global configuration command.

You can combine the commands described in this section to prioritize traffic by placing packets with particular DSCPs or 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. For configuration information, see the “Configuring Ingress Queue Characteristics” section on page 34-72.

### Queueing and Scheduling on Egress Queues

Figure 34-9 shows the queueing and scheduling flowchart for egress ports.

**Note**

If the expedite queue is enabled, SRR services it until it is empty before servicing the other three queues.
Each port supports four egress queues, one of which (queue 1) can be the egress expedite queue. These queues are configured by a queue-set. All traffic leaving an egress port flows through one of these four queues and is subjected to a threshold based on the QoS label assigned to the packet.

Figure 34-10 shows the egress queue buffer. The buffer space is divided between the common pool and the reserved pool. The switch uses a buffer allocation scheme to reserve a minimum amount of buffers for each egress queue, to prevent any queue or port from consuming all the buffers and depriving other queues, and to control whether to grant buffer space to a requesting queue. The switch detects whether the target queue has not consumed more buffers than its reserved amount (under-limit), whether it has consumed all of its maximum buffers (over limit), and whether the common pool is empty (no free
buffers) or not empty (free buffers). If the queue is not over-limit, the switch can allocate buffer space from the reserved pool or from the common pool (if it is not empty). If there are no free buffers in the common pool or if the queue is over-limit, the switch drops the frame.

**Figure 34-10  Egress Queue Buffer Allocation**

![Egress Queue Buffer Allocation Diagram]

**Buffer and Memory Allocation**

You guarantee the availability of buffers, set drop thresholds, and configure the maximum memory allocation for a queue-set by using the `mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` global configuration command. Each threshold value is a percentage of the queue’s allocated memory, which you specify by using the `mls qos queue-set output qset-id buffers allocation1 ... allocation4` global configuration command.

The sum of all the allocated buffers represents the reserved pool, and the remaining buffers are part of the common pool.

Through buffer allocation, you can ensure that high-priority traffic is buffered. For example, if the buffer space is 400, you can allocate 70 percent of it to queue 1 and 10 percent to queues 2 through 4. Queue 1 then has 280 buffers allocated to it, and queues 2 through 4 each have 40 buffers allocated to them.

You can guarantee that the allocated buffers are reserved for a specific queue in a queue-set. For example, if there are 100 buffers for a queue, you can reserve 50 percent (50 buffers). The switch returns the remaining 50 buffers to the common pool. You also can enable a queue in the full condition to obtain more buffers than are reserved for it by setting a maximum threshold. The switch can allocate the needed buffers from the common pool if the common pool is not empty.

**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. You map a port to queue-set by using the `queue-set qset-id` interface configuration command.
Modify the queue-set configuration to change the WTD threshold percentages. For more information about how WTD works, see the “Weighted Tail Drop” section on page 34-14.

**Shaped or Shared Mode**

SRR services each queue-set in shared or shaped 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 commands. For an explanation of the differences between shaping and sharing, see the “SRR Shaping and Sharing” section on page 34-15.

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 DSCPs or 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. For configuration information, see the “Configuring Egress Queue Characteristics” section on page 34-77.

---

**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.

**Packet Modification**

A packet is classified, policed, and queued to provide QoS. Packet modifications can occur during this process:

- 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. The reason for this is that QoS classification and forwarding lookups occur in parallel, and it is possible that the packet is forwarded with its original DSCP to the CPU where it is again processed through software.

- 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 the mutation 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.
Configuring Auto-QoS

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 ingress and 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 use auto-QoS commands to identify ports connected to these Cisco devices:
- Cisco IP Phones
- Devices running the Cisco SoftPhone application
- Cisco TelePresence
- Cisco IP Camera

You also use the 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

These sections contain this configuration information:
- Generated Auto-QoS Configuration, page 34-21
- Effects of Auto-QoS on the Configuration, page 34-31
- Auto-QoS Configuration Guidelines, page 34-31
- Upgrading from Cisco IOS Release 12.2(20)SE or Earlier, page 34-32
- Enabling Auto-QoS, page 34-33

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 Table 34-5.)
- 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

- 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).

The switch configures ingress and egress queues on the port according to the settings in Table 34-2 and Table 34-3.

**Table 34-2: Traffic Types, Packet Labels, and Queues**

<table>
<thead>
<tr>
<th></th>
<th>VoIP Data Traffic</th>
<th>VoIP Control Traffic</th>
<th>Routing Protocol Traffic</th>
<th>STP BPDU Traffic</th>
<th>Real-Time Video Traffic</th>
<th>All Other Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
<td>46</td>
<td>24, 26</td>
<td>48</td>
<td>56</td>
<td>34</td>
<td>–</td>
</tr>
<tr>
<td>CoS</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>3</td>
<td>–</td>
</tr>
<tr>
<td>CoS-to-Ingress Queue Map</td>
<td>4, 5 (queue 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0, 1, 2, 3, 6, 7 (queue 1)</td>
</tr>
<tr>
<td>CoS-to-Egress Queue Map</td>
<td>4, 5 (queue 1)</td>
<td>2, 3, 6, 7 (queue 2)</td>
<td></td>
<td>0 (queue 3)</td>
<td>2 (queue 3)</td>
<td>0, 1 (queue 4)</td>
</tr>
</tbody>
</table>

1. VoIP = voice over IP

**Table 34-3: Auto-QoS Configuration for the Ingress Queues**

<table>
<thead>
<tr>
<th>Ingress Queue</th>
<th>Queue Number</th>
<th>CoS-to-Queue Map</th>
<th>Queue Weight (Bandwidth)</th>
<th>Queue (Buffer) Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRR shared</td>
<td>1</td>
<td>0, 1, 2, 3, 6, 7</td>
<td>70 percent</td>
<td>90 percent</td>
</tr>
<tr>
<td>Priority</td>
<td>2</td>
<td>4, 5</td>
<td>30 percent</td>
<td>10 percent</td>
</tr>
</tbody>
</table>
Chapter 34      Configuring QoS

### Table 34-4   Auto-QoS Configuration for the Egress Queues

<table>
<thead>
<tr>
<th>Egress Queue</th>
<th>Queue Number</th>
<th>CoS-to-Queue Map</th>
<th>Queue Weight (Bandwidth)</th>
<th>Queue (Buffer) Size for Gigabit-Capable Ports</th>
<th>Queue (Buffer) Size for 10/100 Ethernet Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>1</td>
<td>4, 5</td>
<td>up to 100 percent</td>
<td>25 percent</td>
<td>15 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>2</td>
<td>2, 3, 6, 7</td>
<td>10 percent</td>
<td>25 percent</td>
<td>25 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>3</td>
<td>0</td>
<td>60 percent</td>
<td>25 percent</td>
<td>40 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>4</td>
<td>1</td>
<td>20 percent</td>
<td>25 percent</td>
<td>20 percent</td>
</tr>
</tbody>
</table>

For information about the trusted boundary feature, see the “Configuring a Trusted Boundary to Ensure Port Security” section on page 39-42.

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 Table 34-5 to the port.

### Enhanced Auto-QoS for Video, Trust, and Classification

**Note**

The enhanced auto-QoS feature is not supported on switches running LAN Lite images.

In Cisco IOS Release 12.2(55)SE, auto-QoS is enhanced to support video. Automatic configurations are generated that classify and trust traffic from Cisco TelePresence systems and Cisco IP cameras.

When you configure the `auto qos { video | classify | trust }` enhanced commands on a switch port, this behavior occurs:

- **Auto qos voip** generated commands that you configured on the interface before Cisco IOS Release 12.2(55)SE migrate to the enhanced commands.
- Global values change with the migration of enhanced commands. For a complete list of the generated commands that are applied to the running configuration see Table 34-5.

### Auto-QoS Configuration Migration

Auto-QoS configuration migration from legacy auto-QoS to enhanced auto-QoS occurs when:

- A switch is booted with the Cisco IOS Release 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.

| Description | Automatically Generated Command (voip) | Enhanced Automatically Generated Command (Video|Trust|Classify) |
|-------------|---------------------------------------|-----------------------------------------------|
| The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value). | Switch(config)# mls qos \n Switch(config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56 | Switch(config)# mls qos \n Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56 |
| The switch automatically maps CoS values to an ingress queue and to a threshold ID. | Switch(config)# no mls qos srr-queue \n input cos-map \n Switch(config)# mls qos srr-queue \n input cos-map queue 1 threshold 2 1 \n Switch(config)# mls qos srr-queue \n input cos-map queue 1 threshold 3 0 \n Switch(config)# mls qos srr-queue \n input cos-map queue 2 threshold 1 2 \n Switch(config)# mls qos srr-queue \n input cos-map queue 2 threshold 2 4 6 7 \n Switch(config)# mls qos srr-queue \n input cos-map queue 2 threshold 3 5 | Switch(config)# no mls qos srr-queue \n input cos-map \n Switch(config)# mls qos srr-queue \n input cos-map queue 1 threshold 2 3 \n Switch(config)# mls qos srr-queue \n input cos-map queue 1 threshold 3 6 7 \n Switch(config)# mls qos srr-queue \n input cos-map queue 2 threshold 1 4 |
| The switch automatically maps CoS values to an egress queue and to a threshold ID. | Switch(config)# no mls qos srr-queue \n output cos-map \n Switch(config)# mls qos srr-queue \n output cos-map queue 1 threshold 3 5 \n Switch(config)# mls qos srr-queue \n output cos-map queue 2 threshold 3 3 6 7 \n Switch(config)# mls qos srr-queue \n output cos-map queue 3 threshold 3 2 4 \n Switch(config)# mls qos srr-queue \n output cos-map queue 4 threshold 2 1 \n Switch(config)# mls qos srr-queue \n output cos-map queue 4 threshold 3 0 | Switch(config)# no mls qos srr-queue \n output cos-map \n Switch(config)# mls qos srr-queue \n output cos-map queue 1 threshold 3 4 5 \n Switch(config)# mls qos srr-queue \n output cos-map queue 2 threshold 3 6 7 \n Switch(config)# mls qos srr-queue \n output cos-map queue 2 threshold 1 2 \n Switch(config)# mls qos srr-queue \n output cos-map queue 3 threshold 3 0 \n Switch(config)# mls qos srr-queue \n output cos-map queue 4 threshold 3 1 |
The switch automatically maps DSCP values to an ingress queue and to a threshold ID.

Table 34-5  Generated Auto-QoS Configuration (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Automatically Generated Command (voip)</th>
</tr>
</thead>
</table>
| The switch automatically maps DSCP values to an ingress queue and to a threshold ID. | Switch(config)# no mls qos srr-queue input dscp-map
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 32
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 40
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47 |
| Enhanced Automatically Generated Command(Video|Trust|Classify) | Switch(config)# no mls qos srr-queue input dscp-map
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 24
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 52 53 54 55 56
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 57 58 59 60 61 62 63
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 42 43 44 45
Switch(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 46 47 |
### Chapter 34 Configuring QoS

#### Configuring Auto-QoS

The switch automatically maps DSCP values to an egress queue and to a threshold ID.

| Description | Automatically Generated Command (voip) | Enhanced Automatically Generated Command (Video|Trust|Classify) |
|-------------|----------------------------------------|-----------------------------------------------|
| The switch automatically maps DSCP values to an egress queue and to a threshold ID. | Switch(config)# no mls qos srr-queue output dscp-map Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47 | Switch(config)# no mls qos srr-queue output dscp-map Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 41 42 43 44 45 46 47 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35 36 37 38 39 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 2 24 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55 Switch(config)# mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63 Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23 Switch(config)# mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 1 8 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15 Switch(config)# mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7 | |
Table 34-5  Generated Auto-QoS Configuration (continued)

| Description                                                                 | Automatically Generated Command (voip)                                                                 | Enhanced Automatically Generated Command (Video|Trust|Classify)                                                                 |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| The switch automatically sets up the ingress queues, with queue 2 as the  | Switch(config)# no mls qos srr-queue input priority-queue 1                                           | Switch(config)# no mls qos srr-queue input priority-queue 1                                           |
| priority queue and queue 1 in shared mode. The switch also configures the bandwidth and buffer size for the ingress queues. | Switch(config)# no mls qos srr-queue input priority-queue 2                                           | Switch(config)# no mls qos srr-queue input bandwidth 90 10                                          |
|                                                                             | Switch(config)# mls qos srr-queue input bandwidth 2 138 92 400                                        | Switch(config)# mls qos srr-queue input threshold 1 8 16                                              |
|                                                                             | Switch(config)# mls qos srr-queue input threshold 2 138 92 400                                        | Switch(config)# mls qos srr-queue input threshold 1 80 90                                             |
|                                                                             | Switch(config)# mls qos srr-queue input buffers 67 33                                                | Switch(config)# mls qos queue-set output 1 threshold 1 138 138 92 138                               |
|                                                                             |                                                                                                       | Switch(config)# mls qos queue-set output 1 threshold 2 118 118 100 235                              |
|                                                                             |                                                                                                       | Switch(config)# mls qos queue-set output 2 threshold 3 41 68 100 272                                 |
|                                                                             |                                                                                                       | Switch(config)# mls qos queue-set output 2 threshold 4 42 72 100 242                                 |
|                                                                             |                                                                                                       | Switch(config)# mls qos queue-set output 1 buffers 10 10 26 52                                      |
|                                                                             |                                                                                                       | Switch(config)# mls qos queue-set output 2 buffers 16 6 17 61                                      |
|                                                                             |                                                                                                       | Switch(config-if)# priority-queue out                                                                  |
|                                                                             |                                                                                                       | Switch(config-if)# srr-queue                                                                            |
|                                                                             |                                                                                                       | bandwidth share 10 10 60 20                                                                           |
|                                                                             |                                                                                                       |                                                                                                       |
| The switch automatically configures the egress queue buffer sizes. It configures the bandwidth and the SRR mode (shaped or shared) on the egress queues mapped to the port. | Switch(config)# mls qos queue-set output 1 threshold 1 138 138 92 138                               | Switch(config)# mls qos queue-set output 1 threshold 1 100 100 50 200                              |
|                                                                             | Switch(config)# mls qos queue-set output 1 threshold 2 118 118 100 235                              | Switch(config)# mls qos queue-set output 1 threshold 2 125 125 100 400                              |
|                                                                             | Switch(config)# mls qos queue-set output 2 threshold 3 41 68 100 272                                 | Switch(config)# mls qos queue-set output 1 threshold 3 100 100 100 400                              |
|                                                                             | Switch(config)# mls qos queue-set output 2 threshold 4 42 72 100 242                                 | Switch(config)# mls qos queue-set output 1 threshold 4 60 150 50 200                                |
|                                                                             | Switch(config)# mls qos queue-set output 1 buffers 10 10 26 52                                      |                                                                                                       |
|                                                                             | Switch(config)# mls qos queue-set output 2 buffers 16 6 17 61                                      |                                                                                                       |
|                                                                             | Switch(config-if)# priority-queue out                                                                  |                                                                                                       |
|                                                                             | Switch(config-if)# srr-queue                                                                            |                                                                                                       |
|                                                                             | bandwidth share 10 10 60 20                                                                           |                                                                                                       |

Auto-QoS Generated Configuration For VoIP Devices

If you entered the `auto qos voip cisco-phone` command, the switch automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP Phone.

Switch(config-if)# mls qos trust device cisco-phone

If you entered the `auto qos voip cisco-softphone` command, the switch automatically creates class maps and policy maps.

Switch(config)# mls qos map policied-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config-cmap)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Policy-SoftPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 320000 8000 exceed-action policied-dscp-transmit
After creating the class maps and policy maps, the switch automatically applies the policy map called `AutoQoS-Police-SoftPhone` to an ingress interface on which auto-QoS with the Cisco SoftPhone feature is enabled.

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

If you entered the `auto qos voip cisco-phone` command, the switch automatically creates class maps and policy maps.

```
Switch(config-if)# mls qos trust device cisco-phone
```

If you entered the `auto qos voip cisco-softphone` command, the switch automatically creates class maps and policy maps.

```
Switch(config)# mls qos map policed-dscp 24 26 46 to 0
Switch(config)# class-map match-all AutoQoS-VoIP-RTP-Trust
Switch(config-cmap)# match ip dscp ef
Switch(config)# class-map match-all AutoQoS-VoIP-Control-Trust
Switch(config-cmap)# match ip dscp cs3 af31
Switch(config)# policy-map AutoQoS-Police-CiscoPhone
Switch(config-pmap)# class AutoQoS-VoIP-RTP-Trust
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# class AutoQoS-VoIP-Control-Trust
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
```

After creating the class maps and policy maps, the switch automatically applies the policy map called `AutoQoS-Police-SoftPhone` to an ingress interface on which auto-QoS with the Cisco SoftPhone feature is enabled.

```
Switch(config-if)# service-policy input AutoQoS-Police-SoftPhone
```

### Auto-QoS Generated Configuration For Enhanced Video, Trust, and Classify Devices

If you entered these enhanced auto-QoS commands, the switch automatically configures the 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 trust`
- `auto qos trust cos`
- `auto qos trust dscp`

```
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

No class maps and policy maps are configured.
If you entered the `auto qos classify` command, the switch automatically creates class maps and policy maps.

```
Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
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_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCLAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# set dscp af11
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# set dscp default
```

If you entered the `auto qos classify police` command, the switch automatically creates class maps and policy maps.

```
Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
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_BULK_DATA_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-BULK-DATA
Switch(config)# class-map match-all AUTOQOS_SCLAVANGER_CLASS
Switch(config-cmap)# match access-group name AUTOQOS-ACL-SCAVANGER
Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap)# set dscp af11
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# set dscp default

Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
```

Switch(config)# class-map match-all AUTOQOS_BULK_DATA_CLASS
Switch(config-cmap-c)# set dscp af11
Switch(config-pmap-c)# set dscp af11
Switch(config-pmap-c)# set dscp af21
Switch(config-pmap-c)# set dscp cs1
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# set dscp default

; Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action drop
Switch(config-pmap-c)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
Switch(config-if)# service-policy input AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY

This is the enhanced configuration for the auto qos voip cisco-phone command:

Switch(config)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
Switch(config)# class-map match-all AUTOQOS_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
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_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
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-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# class AUTOQOS_DEFAULT_CLASS
Switch(config-pmap-c)# set dscp default
Switch(config-pmap-c)# police 10000000 8000 exceed-action policed-dscp-transmit
;
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)# mls qos map policed-dscp 0 10 18 to 8
Switch(config)# mls qos map cos-dscp 0 8 16 24 32 46 48 56
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_VOIP_DATA_CLASS
Switch(config-cmap)# match ip dscp ef
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_VOIP_SIGNAL_CLASS
Switch(config-cmap)# match ip dscp cs3
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-SOFTPHONE-POLICY
Switch(config-pmap)# class AUTOQOS_VOIP_DATA_CLASS
Switch(config-pmap-c)# set dscp ef
Switch(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# class AUTOQOS_VOIP_SIGNAL_CLASS
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# class AUTOQOS_MULTIENHANCED_CONF_CLASS
Switch(config-pmap-c)# set dscp af41
Switch(config-pmap-c)# police 5000000 8000 exceed-action drop
Switch(config-pmap-c)# class AUTOQOS_BULK_DATA_CLASS
Effects of Auto-QoS on the 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 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.

Auto-QoS Configuration Guidelines

Before configuring auto-QoS, 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](image)

  In releases earlier than Cisco IOS Release 12.2(20)SE, auto-QoS configures VoIP only on switch ports with Cisco IP Phones.

- When a device running Cisco SoftPhone is connected to a nonrouted or routed port, the switch supports only one Cisco SoftPhone application per port.

- Beginning with Cisco IOS Release 12.2(40)SE, Auto-QoS VoIP uses the `priority-queue` interface configuration command for an egress interface. You can also configure a policy-map and trust device on the same interface for Cisco IP phones.

- If the switch port was configure by using the `auto qos voip cisco-phone` interface configuration command in Cisco IOS Release 12.2(37)SE or earlier, the auto-QoS generated commands new to Cisco IOS Release 12.2(40)SE are not applied to the port. To have these commands automatically applied, you must remove and then reapply the configuration to the port.

- 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. For more information, see the Effects of...

- After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes AutoQoS in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. 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.

- 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 the CDP.

- 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

- The auto qos srnd4 global configuration command is generated as a result of enhanced auto-QoS configuration.

- If the legacy auto qos voip commands are executed on the switch and the mls qos command is disabled, the enhanced auto-QoS configuration is generated. Otherwise, legacy auto-QoS commands are executed.

Upgrading from Cisco IOS Release 12.2(20)SE or Earlier

In Cisco IOS Release 12.2(20)SE, the implementation for auto-QoS changed from the previous release. The generated auto-QoS configuration was changed, support for the Cisco SoftPhone feature was added, and support for Cisco IP Phones on routed ports was added.

If auto-QoS is configured on the switch, your switch is running a release earlier than Cisco IOS Release 12.2(20)SE, and you upgrade to Cisco IOS Release 12.2(20)SE or later, the configuration file will not contain the new configuration, and auto-QoS will not operate. Follow these steps to update the auto-QoS settings in your configuration file:

1. Upgrade your switch to Cisco IOS Release 12.2(20)SE or later.
2. Disable auto-QoS on all ports on which auto-QoS was enabled.
3. Return all the global auto-QoS settings to their default values by using the no commands.
4. Re-enable auto-QoS on the ports on which auto-QoS was disabled in Step 2. Configure the ports with the same auto-QoS settings as the previous ones.
Configuring Auto-QoS

For optimum QoS performance, enable auto-QoS on all the devices in your network.

Beginning in privileged EXEC mode, follow these steps to enable auto-QoS devices within a QoS domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify 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 enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| 3     | auto qos voip {cisco-phone |cisco-softphone | trust} or auto qos video {cts | ip-camera} or auto qos classify [police] or auto qos trust {cos | dscp} | Enable auto-QoS. The keywords have these meanings:  
  • cisco-phone—If the port is connected to a Cisco IP Phone, the QoS labels of incoming packets are trusted only when the telephone is detected.  
  • cisco-softphone—The port is connected to device running the Cisco SoftPhone feature.  
  • trust—The uplink port is connected to a trusted switch or router, and the VoIP traffic classification.  
  QoS labels of incoming packets are trusted only when the system is detected.  
  • cts—A port connected to a Cisco Telepresence system.  
  • ip-camera—A port connected to an IP camera.  
  • police—Policing is set up by defining the QoS policy maps and applying them to ports (port-based QoS).  
  • cos—Class of service.  
  • dscp—Differentiated Services Code Point. |
| 4     | exit                           | Return to global configuration mode.                                    |
| 5     | interface interface-id         | Specify the switch port identified as connected to a trusted switch or router, and enter interface configuration mode. |
| 6     | auto qos trust                 | Enable auto-QoS on the port, and specify that the port is connected to a trusted router or switch. |
| 7     | end                            | Return to privileged EXEC mode.                                         |
| 8     | show auto qos interface interface-id | Verify 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. |
Troubleshooting Auto QoS Commands

To display the QoS commands that are automatically generated when auto-QoS is enabled or disabled, enter the `debug auto qos` privileged EXEC command before you enable auto-QoS. For more information, see the `debug autoqos` 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).

You can use the `no mls qos` global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

Displaying Auto-QoS Information

To display the initial auto-QoS configuration, use the `show auto qos [interface [interface-id]]` privileged EXEC command. To display any user changes to that configuration, use the `show running-config` privileged EXEC command. You can compare the `show auto qos` and the `show running-config` command output to identify the user-defined QoS settings.

To display information about the QoS configuration that might be affected by auto-QoS, use one of these commands:

- `show mls qos`
- `show mls qos maps cos-dscp`
- `show mls qos interface [interface-id] [buffers | queueing]`
- `show mls qos maps [cos-dscp | cos-input-q | cos-output-q | dscp-cos | dscp-input-q | dscp-output-q]`
- `show mls qos input-queue`
- `show running-config`

Configuring Standard 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. 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.
These sections contain this configuration information:

- Default Standard QoS Configuration, page 34-35
- Standard QoS Configuration Guidelines, page 34-37
- Enabling QoS Globally, page 34-40 (required)
- Enabling VLAN-Based QoS on Physical Ports, page 34-40 (optional)
- Configuring Classification Using Port Trust States, page 34-41 (required)
- Configuring a QoS Policy, page 34-47 (required)
- Configuring DSCP Maps, page 34-66 (optional, unless you need to use the DSCP-to-DSCP-mutation map or the policed-DSCP map)
- Configuring Ingress Queue Characteristics, page 34-72 (optional)
- Configuring Egress Queue Characteristics, page 34-77 (optional)

**Default Standard QoS Configuration**

QoS is disabled. There is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

When QoS is enabled with 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. The default ingress and egress queue settings are described in the “Default Ingress Queue Configuration” section on page 34-35 and the “Default Egress Queue Configuration” section on page 34-36.

**Default Ingress Queue Configuration**

Table 34-6 shows the default ingress queue configuration when QoS is enabled.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Queue 1</th>
<th>Queue 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer allocation</td>
<td>90 percent</td>
<td>10 percent</td>
</tr>
<tr>
<td>Bandwidth allocation 1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Priority queue bandwidth 2</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>WTD drop threshold 1</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>WTD drop threshold 2</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
</tbody>
</table>

1. The bandwidth is equally shared between the queues. SRR sends packets in shared mode only.
2. Queue 2 is the priority queue. SRR services the priority queue for its configured share before servicing the other queue.
Table 34-7 shows the default CoS input queue threshold map when QoS is enabled.

**Table 34-7**  Default CoS Input Queue Threshold Map

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–4</td>
<td>1–1</td>
</tr>
<tr>
<td>5</td>
<td>2–1</td>
</tr>
<tr>
<td>6, 7</td>
<td>1–1</td>
</tr>
</tbody>
</table>

Table 34-8 shows the default DSCP input queue threshold map when QoS is enabled.

**Table 34-8**  Default DSCP Input Queue Threshold Map

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–39</td>
<td>1–1</td>
</tr>
<tr>
<td>40–47</td>
<td>2–1</td>
</tr>
<tr>
<td>48–63</td>
<td>1–1</td>
</tr>
</tbody>
</table>

**Default Egress Queue Configuration**

Table 34-9 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.

**Table 34-9**  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>100 percent</td>
<td>200 percent</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>WTD drop threshold 2</td>
<td>100 percent</td>
<td>200 percent</td>
<td>100 percent</td>
<td>100 percent</td>
</tr>
<tr>
<td>Reserved threshold</td>
<td>50 percent</td>
<td>50 percent</td>
<td>50 percent</td>
<td>50 percent</td>
</tr>
<tr>
<td>Maximum threshold</td>
<td>400 percent</td>
<td>400 percent</td>
<td>400 percent</td>
<td>400 percent</td>
</tr>
<tr>
<td>SRR shaped weights (absolute) 1</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SRR shared weights 2</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
</tbody>
</table>

1. A shaped weight of zero means that this queue is operating in shared mode.
2. One quarter of the bandwidth is allocated to each queue.
Table 34-10 shows the default CoS output queue threshold map when QoS is enabled.

**Table 34-10  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>

Table 34-11 shows the default DSCP output queue threshold map when QoS is enabled.

**Table 34-11  Default DSCP Output Queue Threshold Map**

<table>
<thead>
<tr>
<th>DSCP Value</th>
<th>Queue ID–Threshold ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0–15</td>
<td>2–1</td>
</tr>
<tr>
<td>16–31</td>
<td>3–1</td>
</tr>
<tr>
<td>32–39</td>
<td>4–1</td>
</tr>
<tr>
<td>40–47</td>
<td>1–1</td>
</tr>
<tr>
<td>48–63</td>
<td>4–1</td>
</tr>
</tbody>
</table>

**Default Mapping Table Configuration**

The default CoS-to-DSCP map is shown in Table 34-12 on page 34-67.
The default IP-precedence-to-DSCP map is shown in Table 34-13 on page 34-68.
The default DSCP-to-CoS map is shown in Table 34-14 on page 34-70.
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).

**Standard QoS Configuration Guidelines**

Before beginning the QoS configuration, you should be aware of this information in these sections:

- “QoS ACL Guidelines” section on page 34-38
- “Applying QoS on Interfaces” section on page 34-38
- “Policing Guidelines” section on page 34-39
- “General QoS Guidelines” section on page 34-39
QoS ACL Guidelines

- 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.
- A trust statement in a policy map requires multiple TCAM entries per ACL line. If an input service policy map contains a trust statement in an ACL, the access-list might be too large to fit into the available QoS TCAM and an error can occur when you apply the policy map to a port. Whenever possible, you should minimize the number of lines in a QoS ACL.

Applying QoS on Interfaces

These guidelines apply to configuring QoS on physical ports and SVIs (Layer 3 interfaces):

- You can configure QoS on physical ports and SVIs. When configuring QoS on physical ports, you create and apply nonhierarchical policy maps. When configuring QoS on SVIs, you can create and apply nonhierarchical and hierarchical policy maps.
- Incoming traffic is classified, policed, and marked down (if configured) regardless of whether the traffic is bridged, routed, or sent to the CPU. It is possible for bridged frames to be dropped or to have their DSCP and CoS values modified.
- Follow these guidelines when configuring policy maps on physical ports or SVIs:
  - You cannot apply the same policy map to a physical port and to an SVI.
  - If VLAN-based QoS is configured on a physical port, the switch removes all the port-based policy maps on the port. The traffic on this physical port is now affected by the policy map attached to the SVI to which the physical port belongs.
  - In a hierarchical policy map attached to an SVI, you can only configure an individual policer at the interface level on a physical port to specify the bandwidth limits for the traffic on the port. The ingress port must be configured as a trunk or as a static-access port. You cannot configure policers at the VLAN level of the hierarchical policy map.
  - The switch does not support aggregate policers in hierarchical policy maps.
  - After the hierarchical policy map is attached to an SVI, the interface-level policy map cannot be modified or removed from the hierarchical policy map. A new interface-level policy map also cannot be added to the hierarchical policy map. If you want these changes to occur, the hierarchical policy map must first be removed from the SVI. You also cannot add or remove a class map specified in the hierarchical policy map.
Policing Guidelines

- The port ASIC device, which controls more than one physical port, supports 256 policers (255 user-configurable policers plus 1 policer reserved for system internal use). The maximum number of user-configurable policers supported per port is 63. For example, you could configure 32 policers on a Gigabit Ethernet port and 8 policers on a Fast Ethernet port, or you could configure 64 policers on a Gigabit Ethernet port and 5 policers on a Fast Ethernet port. Policers are allocated on demand by the software and are constrained by the hardware and ASIC boundaries. You cannot reserve policers per port; there is no guarantee that a port will be assigned to any policer.

- Only one policer is applied to a packet on an ingress port. Only the average rate and committed burst parameters are configurable.

- You can create an aggregate policer that is shared by multiple traffic classes within the same nonhierarchical policy map. However, you cannot use the aggregate policer across different policy maps.

- 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 general QoS guidelines:

- Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch are subject to all ingress QoS processing.

- You are likely to lose data when you change queue settings; therefore, try to make changes when traffic is at a minimum.

A switch that is running the IP services image supports QoS DSCP and IP precedence matching in policy-based routing (PBR) route maps with these limitations:

- You cannot apply QoS DSCP mutation maps and PBR route maps to the same interface.

- You cannot configure DSCP transparency and PBR DSCP route maps on the same switch.
Enabling QoS Globally

By default, QoS is disabled on the switch.

Beginning in privileged EXEC mode, follow these steps to enable QoS. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable QoS, use the `no mls qos` global configuration command.

Enabling VLAN-Based QoS on Physical Ports

By default, VLAN-based QoS is disabled on all physical switch ports. The switch applies QoS, including class maps and policy maps, only on a physical-port basis. You can enable VLAN-based QoS on a switch port.

Beginning in privileged EXEC mode, follow these steps to enable VLAN-based QoS. This procedure is required on physical ports that are specified in the interface level of a hierarchical policy map on an SVI.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>mls qos vlan-based</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mls qos interface interface-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the `no mls qos vlan-based` interface configuration command to disable VLAN-based QoS on the physical port.
Configuring Classification Using Port Trust States

These sections describe how to classify incoming traffic by using port trust states. Depending on your network configuration, you must perform one or more of these tasks or one or more of the tasks in the “Configuring a QoS Policy” section on page 34-47:

- Configuring the Trust State on Ports within the QoS Domain, page 34-41
- Configuring the CoS Value for an Interface, page 34-43
- Configuring a Trusted Boundary to Ensure Port Security, page 34-43
- Enabling DSCP Transparency Mode, page 34-45
- Configuring the DSCP Trust State on a Port Bordering Another QoS Domain, page 34-45

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 34-11 shows a sample network topology.
Beginning in privileged EXEC mode, follow these steps to configure the port to trust the classification of the traffic that it receives:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be trusted, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 mls qos trust [cos</td>
<td>dscp</td>
</tr>
<tr>
<td></td>
<td>The default port is not trusted. If no keyword is specified, the</td>
</tr>
<tr>
<td></td>
<td>default is dscp.</td>
</tr>
<tr>
<td></td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show mls qos interface</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return a port to its untrusted state, use the no mls qos trust interface configuration command.

For information on how to change the default CoS value, see the “Configuring the CoS Value for an Interface” section on page 34-43. For information on how to configure the CoS-to-DSCP map, see the “Configuring the CoS-to-DSCP Map” section on page 34-67.
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</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specify the port to be configured, and enter interface configuration mode. Valid interfaces include physical ports.</td>
</tr>
<tr>
<td>`mls qos cos {default-cos</td>
<td>Configure the default CoS value for the port.</td>
</tr>
<tr>
<td>override}`</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• For <code>default-cos</code>, 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.</td>
</tr>
<tr>
<td></td>
<td>• Use the <code>override</code> 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 <code>override</code> 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, CoS, or IP precedence, 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.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>show mls qos interface</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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, as shown in Figure 34-11 on page 34-41, 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 IEEE 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.

In some situations, you can prevent a PC connected to the Cisco IP Phone from taking advantage of a high-priority data queue. You can use the `switchport priority extend cos` interface configuration command to configure the telephone through the switch CLI to override the priority of the traffic received from the PC.

Beginning in privileged EXEC mode, follow these steps to enable trusted boundary on a port:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 cdp run</td>
<td>Enable CDP globally. By default, CDP is enabled.</td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Specify the port connected to the Cisco IP Phone, and enter interface configuration mode. Valid interfaces include physical ports.</td>
</tr>
<tr>
<td>Step 4 cdp enable</td>
<td>Enable CDP on the port. By default, CDP is enabled.</td>
</tr>
</tbody>
</table>
| Step 5 mls qos trust cos         | Configure the switch port to trust the CoS value in traffic received from the Cisco IP Phone.  
|                                 | or                                                                      |
|                                 | mls qos trust dscp                                                      | Configure the routed port to trust the DSCP value in traffic received from the Cisco IP Phone.  
|                                 | By default, the port is not trusted.                                    |
| Step 6 mls qos trust device cisco-phone | Specify that the Cisco IP Phone is a trusted device.                  |
|                                 | You cannot enable both trusted boundary and auto-QoS (auto qos voip interface configuration command) at the same time; they are mutually exclusive. |
| Step 7 end                       | Return to privileged EXEC mode.                                          |
| Step 8 show mls qos interface    | Verify your entries.                                                    |
| Step 9 copy running-config startup-config | (Optional) Save your entries in the configuration file.                 |

To disable the trusted boundary feature, use the `no mls qos trust device` interface configuration command.
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, and the DSCP-to-DSCP mutation map.

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.

**Note**
Enabling DSCP transparency does not affect the port trust settings on IEEE 802.1Q tunneling ports.

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.

Beginning in privileged EXEC mode, follow these steps to enable DSCP transparency on a switch:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos</td>
</tr>
<tr>
<td>Step 3</td>
<td>no mls qos rewrite ip dscp</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mls qos interface [interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.

**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 as shown in Figure 34-12. Then 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.
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>mls qos map dscp-mutation</strong></td>
</tr>
<tr>
<td><strong>dscp-mutation-name in-dscp to out-dscp</strong></td>
<td>Modify the DSCP-to-DSCP-mutation map.</td>
</tr>
<tr>
<td></td>
<td>The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.</td>
</tr>
<tr>
<td></td>
<td>- For <strong>dscp-mutation-name</strong>, enter the mutation map name. You can create more than one map by specifying a new name.</td>
</tr>
<tr>
<td></td>
<td>- For <strong>in-dscp</strong>, enter up to eight DSCP values separated by spaces.</td>
</tr>
<tr>
<td></td>
<td>Then enter <strong>to</strong> keyword.</td>
</tr>
<tr>
<td></td>
<td>- For <strong>out-dscp</strong>, enter a single DSCP value.</td>
</tr>
<tr>
<td></td>
<td>The DSCP range is 0 to 63.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the port to be trusted, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>mls qos trust dscp</strong></td>
</tr>
<tr>
<td></td>
<td>Configure the ingress port as a DSCP-trusted port. By default, the port is not trusted.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>mls qos dscp-mutation</strong></td>
</tr>
<tr>
<td><strong>dscp-mutation-name</strong></td>
<td>Apply the map to the specified ingress DSCP-trusted port.</td>
</tr>
<tr>
<td></td>
<td>For <strong>dscp-mutation-name</strong>, specify the mutation map name created in Step 2.</td>
</tr>
<tr>
<td></td>
<td>You can configure multiple DSCP-to-DSCP-mutation maps on an ingress port.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>show mls qos maps dscp-mutation</strong></td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To return a port to its non-trusted state, use the **no mls qos trust** interface configuration command. To return to the default DSCP-to-DSCP-mutation map values, use the **no mls qos map dscp-mutation dscp-mutation-name** global configuration command.

This example shows how to configure a port to the DSCP-trusted state and to modify the DSCP-to-DSCP-mutation map (named *gi0/2-mutation*) so that incoming DSCP values 10 to 13 are mapped to DSCP 30:

```text
Switch(config)# mls qos map dscp-mutation gi0/2-mutation 10 11 12 13 to 30
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation gi0/2-mutation
Switch(config-if)# end
```

### Configuring a QoS Policy

Configuring a QoS policy typically requires classifying traffic into classes, configuring policies applied to those traffic classes, and attaching policies to ports.

For background information, see the “Classification” section on page 34-5 and the “Policing and Marking” section on page 34-9. For configuration guidelines, see the “Standard QoS Configuration Guidelines” section on page 34-37.

These sections describe how to classify, police, and mark traffic. Depending on your network configuration, you must perform one or more of these tasks:

- Classifying Traffic by Using ACLs, page 34-48
- Classifying Traffic by Using Class Maps, page 34-51
- Classifying, Policing, and Marking Traffic on SVIs by Using Hierarchical Policy Maps, page 34-57
- Classifying, Policing, and Marking Traffic by Using Aggregate Policers, page 34-64
Classifying Traffic by Using ACLs

You can classify IP traffic by using IP standard or IP extended ACLs; you can classify non-IP traffic by using Layer 2 MAC ACLs.

Beginning in privileged EXEC mode, follow these steps to create an IP standard ACL for IP traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 access-list access-list-number [deny</td>
<td>Create an IP standard ACL, repeating the command as many times as</td>
</tr>
<tr>
<td></td>
<td>• For access-list-number, enter the access list number. The range is</td>
</tr>
<tr>
<td></td>
<td>1 to 99 and 1300 to 1999.</td>
</tr>
<tr>
<td></td>
<td>• Use the permit keyword to permit a certain type of traffic if the</td>
</tr>
<tr>
<td></td>
<td>conditions are matched. Use the deny keyword to deny a certain</td>
</tr>
<tr>
<td></td>
<td>type of traffic if conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• For source, enter the network or host from which the packet is</td>
</tr>
<tr>
<td></td>
<td>being sent. You can use the any keyword as an abbreviation for 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>255.255.255.255.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For source-wildcard, enter the wildcard bits in dotted</td>
</tr>
<tr>
<td></td>
<td>decimal notation to be applied to the source. Place ones in the bit</td>
</tr>
<tr>
<td></td>
<td>positions that you want to ignore.</td>
</tr>
<tr>
<td></td>
<td>Note When creating an access list, remember that, by default, the end</td>
</tr>
<tr>
<td></td>
<td>of the access list contains an implicit deny statement for</td>
</tr>
<tr>
<td></td>
<td>everything if it did not find a match before reaching the end.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show access-lists</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete an access list, use the no access-list access-list-number global configuration command.

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)
```
Beginning in privileged EXEC mode, follow these steps to create an IP extended ACL for IP traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td></td>
<td>Create an IP extended ACL, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td></td>
<td>• For access-list-number, enter the access list number. The range is 100 to 199 and 2000 to 2699.</td>
</tr>
<tr>
<td></td>
<td>• Use the permit keyword to permit a certain type of traffic if the conditions are matched. Use the deny keyword to deny a certain type of traffic if conditions are matched.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show access-lists</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete an access list, use the **no access-list access-list-number** global configuration command.

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
Beginning in privileged EXEC mode, follow these steps to create a Layer 2 MAC ACL for non-IP traffic:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mac access-list extended name</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>{ permit</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• For mask, enter the wildcard bits by placing ones in the bit positions that you want to ignore.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• (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.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show access-lists [access-list-number</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To delete an access list, use the no mac access-list extended access-list-name global configuration command.

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)
Classifying Traffic by Using Class Maps

You use the class-map global configuration command to name and to isolate a specific traffic flow (or class) from all other traffic. The class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as an ACL, IP precedence values, or DSCP values. The match criterion is defined with one match statement entered within the class-map configuration mode.

**Note**
You can also create class-maps during policy map creation by using the class policy-map configuration command. For more information, see the “Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps” section on page 34-53 and the “Classifying, Policing, and Marking Traffic on SVIs by Using Hierarchical Policy Maps” section on page 34-57.

Beginning in privileged EXEC mode, follow these steps to create a class map and to define the match criterion to classify traffic:

<table>
<thead>
<tr>
<th>Command</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> access-list access-list-number { deny</td>
<td>permit} source [source-wildcard]</td>
</tr>
<tr>
<td>or access-list access-list-number { deny</td>
<td>permit} protocol source [source-wildcard] destination [destination-wildcard]</td>
</tr>
<tr>
<td>or mac access-list extended name</td>
<td></td>
</tr>
<tr>
<td>{ permit</td>
<td>deny } { host src-MAC-addr mask</td>
</tr>
<tr>
<td><strong>Step 3</strong> class-map [match-all</td>
<td>match-any] class-map-name</td>
</tr>
<tr>
<td>(Optional) Use the match-all keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched.</td>
<td></td>
</tr>
<tr>
<td>(Optional) Use the match-any keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched.</td>
<td></td>
</tr>
<tr>
<td>For class-map-name, specify the name of the class map. If neither the match-all or match-any keyword is specified, the default is match-all.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Because only one match command per class map is supported, the match-all and match-any keywords function the same.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Standard QoS

#### Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`match {access-group acl-index-or-name</td>
<td>ip dscp dscp-list</td>
</tr>
<tr>
<td><code>no policy-map policy-map-name</code></td>
<td>Remove a policy map.</td>
</tr>
<tr>
<td>`no class-map [match-all</td>
<td>match-any] class-map-name`</td>
</tr>
<tr>
<td>`no match {access-group acl-index-or-name</td>
<td>ip dscp dscp-list</td>
</tr>
</tbody>
</table>

#### Step 5

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

#### Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show class-map</code></td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

#### Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete an existing policy map, use the **no policy-map policy-map-name** global configuration command. To delete an existing class map, use the **no class-map [match-all | match-any] class-map-name** global configuration command. To remove a match criterion, use the **no match {access-group acl-index-or-name | ip dscp dscp-list | ip precedence ip-precedence-list}** class-map configuration command.

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.

```plaintext
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.

```plaintext
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# end
Switch#
```

This example shows how to create a class map called `class3`, which matches incoming traffic with IP-precedence values of 5, 6, and 7.

```plaintext
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# end
Switch#
```
Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions can include trusting the CoS, DSCP, or IP precedence values in the traffic class; setting a specific DSCP or IP precedence value in the traffic class; and specifying the traffic bandwidth limitations for each matched traffic class (policer) and the action to take when the traffic is out of profile (marking).

A policy map also has these characteristics:
- A policy map can contain multiple class statements, each with different match criteria and policers.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.
- A separate policy-map class can exist for each type of traffic received through a port.
- A policy-map trust state and a port trust state are mutually exclusive, and whichever is configured last takes effect.

Follow these guidelines when configuring policy maps on physical ports:
- You can attach only one policy map per ingress port.
- If you configure the IP-precedence-to-DSCP map by using the `mls qos map ip-prec-dscp dscp1...dscp8` global configuration command, the settings only affect packets on ingress interfaces that are configured to trust the IP precedence value. In a policy map, if you set the packet IP precedence value to a new value by using the `set ip precedence new-precedence` policy-map class configuration command, the egress DSCP value is not affected by the IP-precedence-to-DSCP map. If you want the egress DSCP value to be different than the ingress value, use the `set dscp new-dscp` policy-map class configuration command.
- If you enter or have used the `set ip dscp` command, the switch changes this command to `set dscp` in its configuration.
- You can use the `set ip precedence` or the `set precedence` policy-map class configuration command to change the packet IP precedence value. This setting appears as `set ip precedence` in the switch configuration.
- You can configure a separate second-level policy map for each class defined for the port. The second-level policy map specifies the police action to take for each traffic class. For information on configuring a hierarchical policy map, see Classifying, Policing, and Marking Traffic on SVIs by Using Hierarchical Policy Maps, page 34-57.
- A policy-map and a port trust state can both run on a physical interface. The policy-map is applied before the port trust state.
- When you configure a default traffic class by using the `class 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`).
Beginning in privileged EXEC mode, follow these steps to create a nonhierarchial policy map:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**class-map [match-all</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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>policy-map policy-map-name</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**class [class-map-name</td>
</tr>
</tbody>
</table>
### Command Purpose

| Step 5 | trust [cos | dscp | ip-precedence] | Configure the trust state, which QoS uses to generate a CoS-based or DSCP-based QoS label. |
|--------|------------------------|--------------------------------------------------------------------------------------------|
| **Note** | This command is mutually exclusive with the set command within the same policy map. If you enter the **trust** command, go to Step 6. |
| By default, the port is not trusted. If no keyword is specified when the command is entered, the default is **dscp**. |

The keywords have these meanings:
- **cos**—QoS derives the DSCP value by using the received or default port CoS value and the CoS-to-DSCP map.
- **dscp**—QoS derives the DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the default port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.
- **ip-precedence**—QoS derives the DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the default port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.

For more information, see the “Configuring the CoS-to-DSCP Map” section on page 34-67.

| Step 6 | set {dscp new-dscp | ip precedence new-precedence} | Classify IP traffic by setting a new value in the packet. |
|--------|--------------------------------------------|----------------------------------------------------------|
| For **dscp new-dscp**, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63. |
| For **ip precedence new-precedence**, enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7. |

| Step 7 | police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}] | Define a policer for the classified traffic. |
|--------|---------------------------------------------------------------|------------------------------------------------|
| By default, no policer is defined. For information on the number of policers supported, see the “Standard QoS Configuration Guidelines” section on page 34-37. |
| For **rate-bps**, specify average traffic rate in bits per second (b/s). The range is 8000 to 10000000000. |
| For **burst-byte**, specify the normal burst size in bytes. The range is 8000 to 1000000. |
| (Optional) Specify the action to take when the rates are exceeded. Use the **exceed-action drop** keywords to drop the packet. Use the **exceed-action policed-dscp-transmit** keywords to mark down the DSCP value (by using the policed-DSCP map) and to send the packet. For more information, see the “Configuring the Policed-DSCP Map” section on page 34-69. |
To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class map, use the `no class class-map-name` policy-map configuration command. To return to the untrusted state, use the `no trust policy-map configuration` command. To remove an assigned DSCP or IP precedence value, use the `no set {dscp new-dscp | ip precedence new-precedence}` policy-map configuration command. To remove an existing policer, use the `no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]` policy-map configuration command. To remove the policy map and port association, use the `no service-policy input policy-map-name` interface configuration command.

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)# trust dscp
Switch(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-if)# interface gigabitethernet0/1
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
```

**Step 8**
exit

Return to policy map configuration mode.

**Step 9**
exit

Return to global configuration mode.

**Step 10**
interface interface-id

Specify the port to attach to the policy map, and enter interface configuration mode.

Valid interfaces include physical ports.

**Step 11**
service-policy input policy-map-name

Specify the policy-map name, and apply it to an ingress port.

Only one policy map per ingress port is supported.

**Step 12**
end

Return to privileged EXEC mode.

**Step 13**
show policy-map [policy-map-name [class class-map-name]]

Verify your entries.

**Step 14**
copy running-config startup-config

(Optional) Save your entries in the configuration file.
Chapter 34      Configuring QoS

Classifying, Policing, and Marking Traffic on SVIs by Using Hierarchical Policy Maps

You can configure hierarchical policy maps on SVIs, but not on other types of interfaces. Hierarchical policing combines the VLAN- and interface-level policy maps to create a single policy map.

On an SVI, the VLAN-level policy map specifies which traffic class to act on. Actions can include trusting the CoS, DSCP, or IP precedence values or setting a specific DSCP or IP precedence value in the traffic class. Use the interface-level policy map to specify the physical ports that are affected by individual policers.

Follow these guidelines when configuring hierarchical policy maps:

- Before configuring a hierarchical policy map, you must enable VLAN-based QoS on the physical ports that are to be specified at the interface level of the policy map.
- You can attach only one policy map per ingress port or SVI.
- A policy map can contain multiple class statements, each with different match criteria and actions.
- A separate policy-map class can exist for each type of traffic received on the SVI.

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 pm1
Switch(config-pmap)# class cm-1
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# set dscp 6
Switch(config-pmap-c)# exit
Switch(config)# policy-map pm1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config)# interface G0/1
Switch(config-if)# switch mode access
Switch(config-if)# service-policy input pm1
• 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.

• If you configure the IP-precedence-to-DSCP map by using the `mls qos map ip-prec-dscp dscp1...dscp8` global configuration command, the settings only affect packets on ingress interfaces that are configured to trust the IP precedence value. In a policy map, if you set the packet IP precedence value to a new value by using the `set ip precedence new-precedence` policy-map class configuration command, the egress DSCP value is not affected by the IP-precedence-to-DSCP map. If you want the egress DSCP value to be different than the ingress value, use the `set dscp new-dscp` policy-map class configuration command.

• If you enter or have used the `set ip dscp` command, the switch changes this command to `set dscp` in its configuration. If you enter the `set ip dscp` command, this setting appears as `set dscp` in the switch configuration.

• You can use the `set ip precedence` or the `set precedence` policy-map class configuration command to change the packet IP precedence value. This setting appears as `set ip precedence` in the switch configuration.

• If VLAN-based QoS is enabled, the hierarchical policy map supersedes the previously configured port-based policy map.

• The hierarchical policy map is attached to the SVI and affects all traffic belonging to the VLAN. The actions specified in the VLAN-level policy map affect the traffic belonging to the SVI. The police action on the port-level policy map affects the ingress traffic on the affected physical interfaces.

• When configuring a hierarchical policy map on trunk ports, the VLAN ranges must not overlap. If the ranges overlap, the actions specified in the policy map affect the incoming and outgoing traffic on the overlapped VLANs.

• Aggregate policers are not supported in hierarchical policy maps.

• When VLAN-based QoS is enabled, the switch supports VLAN-based features, such as the VLAN map.

• You can configure a hierarchical policy map only on the primary VLAN of a private VLAN.

• 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 default traffic class (`class-default`).
Beginning in privileged EXEC mode, follow these steps to create a hierarchical policy map:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
</tbody>
</table>
| **Step 2** | class-map [match-all | match-any] class-map-name | Create a VLAN-level class map, and enter class-map configuration mode. For information about creating a class map, see the “Classifying Traffic by Using Class Maps” section on page 34-51. By default, no class maps are defined.  
* (Optional) Use the match-all keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched.  
* (Optional) Use the match-any keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched.  
* For class-map-name, specify the name of the class map.  
**Note** Because only one match command per class map is supported, the match-all and match-any keywords function the same. |
| **Step 3** | match {access-group acl-index-or-name | ip dscp dscp-list | ip precedence ip-precedence-list} | Define the match criterion to classify traffic. By default, no match criterion is defined. Only one match criterion per class map is supported, and only one ACL per class map is supported.  
* For access-group acl-index-or-name, specify the number or name of the ACL.  
* For ip dscp dscp-list, enter a list of up to eight IP DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63.  
* For ip precedence ip-precedence-list, enter a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. |
| **Step 4** | exit | Return to class-map configuration mode. |
| **Step 5** | exit | Return to global configuration mode. |
Chapter 34  Configuring QoS

Configuring Standard QoS

Step 6

class-map [match-all | match-any] class-map-name

Create an interface-level class map, and enter class-map configuration mode.

By default, no class maps are defined.

- (Optional) Use the match-all keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched.
- (Optional) Use the match-any keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched.
- For class-map-name, specify the name of the class map.

If neither the match-all or match-any keyword is specified, the default is match-all.

Note Because only one match command per class map is supported, the match-all and match-any keywords function the same.

Step 7

match input-interface interface-id-list

Specify the physical ports on which the interface-level class map acts. You can specify up to six ports as follows:

- A single port (counts as one entry)
- A list of ports separated by a space (each port counts as an entry)
- A range of ports separated by a hyphen (counts as two entries)

This command can only be used in the child-level policy map and must be the only match condition in the child-level policy map.

Step 8

exit

Return to class-map configuration mode.

Step 9

exit

Return to global configuration mode.

Step 10

policy-map policy-map-name

Create an interface-level policy map by entering the policy-map name, and enter policy-map configuration mode.

By default, no policy maps are defined, and no policing is performed.

Step 11

class-map class-map-name

Define an interface-level traffic classification, and enter policy-map configuration mode.

By default, no policy-map class-maps are defined.

If a traffic class has already been defined by using the class-map global configuration command, specify its name for class-map-name in this command.

Command | Purpose
---|---
Step 6 class-map [match-all | match-any] class-map-name | Create an interface-level class map, and enter class-map configuration mode.
Step 7 match input-interface interface-id-list | Specify the physical ports on which the interface-level class map acts. You can specify up to six ports as follows:
- A single port (counts as one entry)
- A list of ports separated by a space (each port counts as an entry)
- A range of ports separated by a hyphen (counts as two entries)
This command can only be used in the child-level policy map and must be the only match condition in the child-level policy map.
Step 8 exit | Return to class-map configuration mode.
Step 9 exit | Return to global configuration mode.
Step 10 policy-map policy-map-name | Create an interface-level policy map by entering the policy-map name, and enter policy-map configuration mode.
By default, no policy maps are defined, and no policing is performed.
Step 11 class-map class-map-name | Define an interface-level traffic classification, and enter policy-map configuration mode.
By default, no policy-map class-maps are defined.
If a traffic class has already been defined by using the class-map global configuration command, specify its name for class-map-name in this command.
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 12     | **police rate-bps burst-byte [exceed-action drop | policed-dscp-transmit]**]                     | Define an individual policer for the classified traffic. By default, no policer is defined. For information on the number of policers supported, see the “Standard QoS Configuration Guidelines” section on page 34-37. For *rate-bps*, specify average traffic rate in bits per second (b/s). The range is 8000 to 10000000000.  
  - For *burst-byte*, specify the normal burst size in bytes. The range is 8000 to 1000000.  
  - (Optional) Specify the action to take when the rates are exceeded. Use the **exceed-action drop** keywords to drop the packet. Use the **exceed-action policed-dscp-transmit** keywords to mark down the DSCP value (by using the policed-DSCP map) and to send the packet. For more information, see the “Configuring the Policed-DSCP Map” section on page 34-69. |
| 13     | exit                                         | Return to policy-map configuration mode.                                                          |
| 14     | exit                                         | Return to global configuration mode.                                                              |
| 15     | **policy-map policy-map-name**               | Create a VLAN-level policy map by entering the policy-map name, and enter policy-map configuration mode. By default, no policy maps are defined. The default behavior of a policy map is to set the DSCP to 0 if the packet is an IP packet and to set the CoS to 0 if the packet is tagged. No policing is performed. |
| 16     | **class [class-map-name | class-default]**                        | Defines a traffic classification, and enter policy-map class configuration mode. By default, no policy map class-maps are defined.  
If a traffic class has already been defined by using the **class-map** global configuration command, specify its name for **class-map-name** in this command.  
A **class-default** traffic class is pre-defined and can be added to any policy. It is always placed at the end of a policy map. With an implied **match any** included in the **class-default** class, all packets that have not already matched the other traffic classes will match **class-default**. |
### Chapter 34 Configuring QoS

#### Configuring Standard QoS

| Step 17 | trust [cos | dscp | ip-precedence] | **Purpose** |
|---------|-----------------------------|-------------|
|         | Configure the trust state, which QoS uses to generate a CoS-based or DSCP-based QoS label. |
| **Note** | This command is mutually exclusive with the `set` command within the same policy map. If you enter the `trust` command, omit Step 18. |

By default, the port is not trusted. If no keyword is specified when the command is entered, the default is `dscp`.

The keywords have these meanings:

- **cos**—QoS derives the DSCP value by using the received or default port CoS value and the CoS-to-DSCP map.
- **dscp**—QoS derives the DSCP value by using the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the default port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.
- **ip-precedence**—QoS derives the DSCP value by using the IP precedence value from the ingress packet and the IP-precedence-to-DSCP map. For non-IP packets that are tagged, QoS derives the DSCP value by using the received CoS value; for non-IP packets that are untagged, QoS derives the DSCP value by using the default port CoS value. In either case, the DSCP value is derived from the CoS-to-DSCP map.

For more information, see the “Configuring the CoS-to-DSCP Map” section on page 34-67.

| Step 18 | set {dscp new-dscp | ip precedence new-precedence} | **Purpose** |
|---------|-----------------------------|-------------|
|         | Classify IP traffic by setting a new value in the packet. |
|         | For `dscp new-dscp`, enter a new DSCP value to be assigned to the classified traffic. The range is 0 to 63. |
|         | For `ip precedence new-precedence`, enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7. |

<table>
<thead>
<tr>
<th>Step 19</th>
<th>service-policy policy-map-name</th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify the interface-level policy-map name (from Step 10) and associate it with the VLAN-level policy map.</td>
<td></td>
</tr>
</tbody>
</table>

If the VLAN-level policy map specifies more than one class, beginning in Cisco IOS Release 12.2(25)SED, each class can have a different `service-policy policy-map-name` command.

<table>
<thead>
<tr>
<th>Step 20</th>
<th>exit</th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Return to policy-map configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 21</th>
<th>exit</th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Return to global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 22</th>
<th>interface interface-id</th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify the SVI to which to attach the hierarchical policy map, and enter interface configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Step 23</th>
<th>service-policy input policy-map-name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify the VLAN-level policy-map name, and apply it to the SVI. Repeat the previous step and this command to apply the policy map to other SVIs. If the hierarchical VLAN-level policy map has more than one interface-level policy map, all class maps must be configured to the same VLAN-level policy map specified in the service-policy policy-map-name command.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 24</th>
<th>end</th>
<th>Return to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 25</td>
<td>show policy-map [policy-map-name [class class-map-name]]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>or show mls qos vlan-based</td>
<td></td>
</tr>
<tr>
<td>Step 26</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete an existing policy map, use the `no policy-map policy-map-name` global configuration command. To delete an existing class map, use the `no class class-map-name` policy-map configuration command.

To return to the untrusted state in a policy map, use the `no trust` policy-map configuration command. To remove an assigned DSCP or IP precedence value, use the `no set {dscp new-dscp | ip precedence new-precedence}` policy-map configuration command.

**Note**

To remove an existing policer in an interface-level policy map, use the `no police rate-bps burst-byte [exceed-action {drop | policed-dscp-transmit}]` policy-map configuration command. To remove the hierarchical policy map and port associations, use the `no service-policy input policy-map-name` interface configuration command.

This example shows how to create a hierarchical policy map:

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list 101 permit ip any any
Switch(config)# class-map cm-1
Switch(config-cmap)# match access 101
Switch(config-cmap)# exit
Switch(config)# exit
Switch#
```

This example shows how to attach the new map to an SVI:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map cm-interface-1
Switch(config-cmap)# match input g3/0/1 - g3/0/2
Switch(config-cmap)# exit
Switch(config)# policy-map port-plcmap
Switch(config-pmap)# class cm-interface-1
Switch(config-pmap-c)# police 900000 9000 exc policed-dscp-transmit
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan-plcmap
Switch(config-pmap)# class cm-1
```
Switch(config-pmap-c)# set dscp 7
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-2
Switch(config-pmap-c)# service-policy port-plcmap-1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# service-policy port-plcmap-2
Switch(config-pmap-c)# set dscp 20
Switch(config-pmap)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust dscp
Switch(config-pmap)# exit
Switch(config)# interface vlan 10
Switch(config-if)# service-policy input vlan-plcmap
Switch(config-if)# exit
Switch(config)# exit

This example shows how to configure default traffic class to a policy map:

Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# match protocol ip
Switch(config-cmap)# exit
Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap)# set dscp 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit
Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# trust cos
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

This example shows how the default traffic class is automatically placed at the end of policy-map pm3 even though class-default was configured first:

Switch# show policy-map pm3
Policy Map pm3
 Class cm-3
   set dscp 4
 Class cm-4
trust cos
 Class class-default
   police 8000 80000 exceed-action drop
Switch#

Classifying, Policing, and Marking Traffic by Using Aggregate Policers

By using an aggregate policer, you can create a policer that is shared by multiple traffic classes within the same policy map. However, you cannot use the aggregate policer across different policy maps or ports.
Beginning in privileged EXEC mode, follow these steps to create an aggregate policer:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mls qos aggregate-policer aggregate-policer-name rate-bps burst-byte exceed-action {drop</td>
</tr>
<tr>
<td></td>
<td>Define the policer parameters that can be applied to multiple traffic classes within the same policy map.</td>
</tr>
<tr>
<td></td>
<td>By default, no aggregate policer is defined. For information on the number of policers supported, see the “Standard QoS Configuration Guidelines” section on page 34-37.</td>
</tr>
<tr>
<td></td>
<td>• For aggregate-policer-name, specify the name of the aggregate policer.</td>
</tr>
<tr>
<td></td>
<td>• For rate-bps, specify average traffic rate in bits per second (b/s). The range is 8000 to 1000000000.</td>
</tr>
<tr>
<td></td>
<td>• For burst-byte, specify the normal burst size in bytes. The range is 8000 to 1000000.</td>
</tr>
<tr>
<td></td>
<td>• Specify the action to take when the rates are exceeded. Use the exceed-action drop keywords to drop the packet. Use the exceed-action policed-dscp-transmit keywords to mark down the DSCP value (by using the policed-DSCP map) and to send the packet. For more information, see the “Configuring the Policed-DSCP Map” section on page 34-69.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>class-map [match-all</td>
</tr>
<tr>
<td></td>
<td>Create a class map to classify traffic as necessary. For more information, see the “Classifying Traffic by Using Class Maps” section on page 34-51.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>policy-map policy-map-name</td>
</tr>
<tr>
<td></td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the “Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps” section on page 34-53.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>class [class-map-name</td>
</tr>
<tr>
<td></td>
<td>Define a traffic classification, and enter policy-map class configuration mode.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the “Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps” section on page 34-53.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>police aggregate aggregate-policer-name</td>
</tr>
<tr>
<td></td>
<td>Apply an aggregate policer to multiple classes in the same policy map.</td>
</tr>
<tr>
<td></td>
<td>For aggregate-policer-name, enter the name specified in Step 2.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td></td>
<td>Specify the port to attach to the policy map, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Valid interfaces include physical ports.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>service-policy input policy-map-name</td>
</tr>
<tr>
<td></td>
<td>Specify the policy-map name, and apply it to an ingress port.</td>
</tr>
<tr>
<td></td>
<td>Only one policy map per ingress port is supported.</td>
</tr>
</tbody>
</table>
To remove the specified aggregate policer from a policy map, use the `no police aggregate aggregate-policer-name` policy map configuration mode. To delete an aggregate policer and its parameters, use the `no mls qos aggregate-policer aggregate-policer-name` global configuration command.

This example shows how to create an aggregate policer and attach it to multiple classes within a policy map. In the configuration, the IP ACLs permit traffic from network 10.1.0.0 and from host 11.3.1.1. For traffic coming from network 10.1.0.0, the DSCP in the incoming packets is trusted. For traffic coming from host 11.3.1.1, the DSCP in the packet is changed to 56. The traffic rate from the 10.1.0.0 network and from host 11.3.1.1 is policed. If the traffic exceeds an average rate of 48000 b/s and a normal burst size of 8000 bytes, its DSCP is marked down (based on the policed-DSCP map) and sent. The policy map is attached to an ingress port.

```
Switch(config)# access-list 1 permit 10.1.0.0 0.0.255.255
Switch(config)# access-list 2 permit 11.3.1.1
Switch(config)# mls qos aggregate-police transmit1 48000 8000 exceed-action policed-dscp-transmit
Switch(config)# class-map ipclass1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map ipclass2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy-map aggflow1
Switch(config-pmap)# class ipclass1
Switch(config-pmap-c)# trust dscp
Switch(config-pmap-c)# police aggregate transmit1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class ipclass2
Switch(config-pmap-c)# set dscp 56
Switch(config-pmap-c)# police aggregate transmit1
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 gigabitethernet0/1
Switch(config-if)# service-policy input aggflow1
Switch(config-if)# exit
```

### Configuring DSCP Maps

These sections contain this configuration information:

- Configuring the CoS-to-DSCP Map, page 34-67 (optional)
- Configuring the IP-Precedence-to-DSCP Map, page 34-68 (optional)
- Configuring the Policed-DSCP Map, page 34-69 (optional, unless the null settings in the map are not appropriate)
• Configuring the DSCP-to-CoS Map, page 34-70 (optional)
• Configuring the DSCP-to-DSCP-Mutation Map, page 34-71 (optional, unless the null settings in the map are not appropriate)

All the maps, except the DSCP-to-DSCP-mutation map, are globally defined and are applied to all ports.

**Configuring the CoS-to-DSCP Map**

You use the CoS-to-DSCP map to map CoS values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic.

Table 34-12 shows the default CoS-to-DSCP map.

<table>
<thead>
<tr>
<th>CoS Value</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the CoS-to-DSCP map. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos map cos-dscp dscp1...dscp8</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos maps cos-dscp</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default map, use the no mls qos cos-dscp global configuration command.

This example shows how to modify and display the CoS-to-DSCP map:

```
Switch(config)# mls qos map cos-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
```
Switch# show mls qos maps cos-dscp

Cos-dscp map:
  cos: 0 1 2 3 4 5 6 7
  dscp: 10 15 20 25 30 35 40 45

Configuring the IP-Precedence-to-DSCP Map

You use the IP-precedence-to-DSCP map to map IP precedence values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic.

Table 34-13 shows the default IP-precedence-to-DSCP map:

<table>
<thead>
<tr>
<th>IP Precedence Value</th>
<th>DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the IP-precedence-to-DSCP map. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos map ip-prec-dscp</td>
<td>Modify the IP-precedence-to-DSCP map.</td>
</tr>
<tr>
<td></td>
<td>dscp1...dscp8</td>
<td>For dscp1...dscp8, enter eight DSCP values that correspond to the IP precedence values 0 to 7. Separate each DSCP value with a space. The DSCP range is 0 to 63.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos maps ip-prec-dscp</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default map, use the no mls qos ip-prec-dscp global configuration command.
This example shows how to modify and display the IP-precedence-to-DSCP map:

```
Switch(config)# mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45
Switch(config)# end
Switch# show mls qos maps ip-prec-dscp

IpPrecedence-dscp map:
<table>
<thead>
<tr>
<th>ipprec:</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp:</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
<td>30</td>
<td>35</td>
<td>40</td>
<td>45</td>
</tr>
</tbody>
</table>
```

### Configuring the Policed-DSCP Map

You use the policed-DSCP map to mark down a DSCP value to a new value as the result of a policing and marking action.

The default policed-DSCP map is a null map, which maps an incoming DSCP value to the same DSCP value.

Beginning in privileged EXEC mode, follow these steps to modify the policed-DSCP map. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos map policed-dscp dscp-list to mark-down-dscp</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos maps policed-dscp</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default map, use the `no mls qos policed-dscp` global configuration command.

This example shows how to map DSCP 50 to 57 to a marked-down DSCP value of 0:

```
Switch(config)# mls qos map policed-dscp 50 51 52 53 54 55 56 57 to 0
Switch(config)# end
Switch# show mls qos maps policed-dscp

Policed-dscp map:
<table>
<thead>
<tr>
<th>d1 : d2</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 :</td>
<td>00</td>
<td>01</td>
<td>02</td>
<td>03</td>
<td>04</td>
<td>05</td>
<td>06</td>
<td>07</td>
<td>08</td>
<td>09</td>
</tr>
<tr>
<td>1 :</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>2 :</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td>3 :</td>
<td>30</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>4 :</td>
<td>40</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td>49</td>
</tr>
<tr>
<td>5 :</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>00</td>
<td>58</td>
<td>59</td>
</tr>
<tr>
<td>6 :</td>
<td>60</td>
<td>61</td>
<td>62</td>
<td>63</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
In this policed-DSCP map, the marked-down DSCP values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the original DSCP; the d2 row specifies the least-significant digit of the original DSCP. The intersection of the d1 and d2 values provides the marked-down value. For example, an original DSCP value of 53 corresponds to a marked-down DSCP value of 0.

**Configuring the DSCP-to-CoS Map**

You use the DSCP-to-CoS map to generate a CoS value, which is used to select one of the four egress queues.

Table 34-14 shows the default DSCP-to-CoS map.

<table>
<thead>
<tr>
<th>Table 34-14</th>
<th>Default DSCP-to-CoS Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP Value</td>
<td>CoS Value</td>
</tr>
<tr>
<td>0–7</td>
<td>0</td>
</tr>
<tr>
<td>8–15</td>
<td>1</td>
</tr>
<tr>
<td>16–23</td>
<td>2</td>
</tr>
<tr>
<td>24–31</td>
<td>3</td>
</tr>
<tr>
<td>32–39</td>
<td>4</td>
</tr>
<tr>
<td>40–47</td>
<td>5</td>
</tr>
<tr>
<td>48–55</td>
<td>6</td>
</tr>
<tr>
<td>56–63</td>
<td>7</td>
</tr>
</tbody>
</table>

If these values are not appropriate for your network, you need to modify them.

Beginning in privileged EXEC mode, follow these steps to modify the DSCP-to-CoS map. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos map dscp-cos dscp-list to cos Modify the DSCP-to-CoS map.</td>
</tr>
<tr>
<td></td>
<td>• For dscp-list, enter up to eight DSCP values separated by spaces. Then enter the to keyword.</td>
</tr>
<tr>
<td></td>
<td>• For cos, enter the CoS value to which the DSCP values correspond. The DSCP range is 0 to 63; the CoS range is 0 to 7.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos maps dscp-to-cos Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default map, use the `no mls qos dscp-cos` global configuration command.
This example shows how to map DSCP values 0, 8, 16, 24, 32, 40, 48, and 50 to CoS value 0 and to display the map:

```
Switch(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 50 to 0
Switch(config)# end
Switch# show mls qos maps dscp-cos
Dscp-cos map:
  d1 :  d2 0  1  2  3  4  5  6  7  8  9
  -------------------------------
  0 :    00 00 00 00 00 00 00 00 00 01
  1 :    01 01 01 01 01 01 00 02 02 02
  2 :    02 02 02 02 00 03 03 03 03 03
  3 :    03 03 00 04 04 04 04 04 04 04
  4 :    00 05 05 05 05 05 05 05 00 06
  5 :    00 06 06 06 06 07 07 07 07 07
  6 :    07 07 07 07
```

Note
In the above DSCP-to-CoS map, the CoS values are shown in the body of the matrix. The d1 column specifies the most-significant digit of the DSCP; the d2 row specifies the least-significant digit of the DSCP. The intersection of the d1 and d2 values provides the CoS value. For example, in the DSCP-to-CoS map, a DSCP value of 08 corresponds to a CoS value of 0.

### Configuring the DSCP-to-DSCP-Mutation Map

If two QoS domains have different DSCP definitions, use the DSCP-to-DSCP-mutation map to translate one set of DSCP values to match the definition of another domain. You apply the DSCP-to-DSCP-mutation map to the receiving port (ingress mutation) at the boundary of a QoS administrative domain.

With ingress mutation, the new DSCP value overwrites the one in the packet, and QoS treats the packet with this new value. The switch sends the packet out the port with the new DSCP value.

You can configure multiple DSCP-to-DSCP-mutation maps on an ingress port. The default DSCP-to-DSCP-mutation map is a null map, which maps an incoming DSCP value to the same DSCP value.

Beginning in privileged EXEC mode, follow these steps to modify the DSCP-to-DSCP-mutation map. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>mls qos map dscp-mutation dscp-mutation-name in-dscp to out-dscp</td>
<td>Modify the DSCP-to-DSCP-mutation map.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For dscp-mutation-name, enter the mutation map name. You can create more than one map by specifying a new name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For in-dscp, enter up to eight DSCP values separated by spaces. Then enter the to keyword.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For out-dscp, enter a single DSCP value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The DSCP range is 0 to 63.</td>
</tr>
<tr>
<td>3</td>
<td>interface interface-id</td>
<td>Specify the port to which to attach the map, and enter interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid interfaces include physical ports.</td>
</tr>
</tbody>
</table>
### Configuring Standard QoS

#### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td><code>mls qos trust dscp</code> Configure the ingress port as a DSCP-trusted port. By default, the port is not trusted.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>mls qos dscp-mutation</code> Apply the map to the specified ingress DSCP-trusted port. For <code>dscp-mutation-name</code>, enter the mutation map name specified in Step 2.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show mls qos maps dscp-mutation</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default map, use the `no mls qos dscp-mutation dscp-mutation-name` global configuration command.

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 mutation1 1 2 3 4 5 6 7 to 0
Switch(config)# mls qos map dscp-mutation mutation1 8 9 10 11 12 13 to 10
Switch(config)# mls qos map dscp-mutation mutation1 20 21 22 to 20
Switch(config)# mls qos map dscp-mutation mutation1 30 31 32 33 34 to 30
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)# mls qos dscp-mutation mutation1
Switch(config-if)# end
Switch# show mls qos maps dscp-mutation mutation1
Dscp-dscp mutation map:
  mutation1:       d1 : d2 0 1 2 3 4 5 6 7 8 9
  -------------------------------
  0 :    00 00 00 00 00 00 00 10 10
  1 :    10 10 10 14 15 16 17 18 19
  2 :    20 20 20 24 25 26 27 28 29
  3 :    30 30 30 30 30 30 30 30 30
  4 :    40 41 42 43 44 45 46 47 48 49
  5 :    50 51 52 53 54 55 56 57 58 59
  6 :    60 61 62 63
```

**Note**

In 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.

### Configuring Ingress Queue Characteristics

Depending on the complexity of your network and your QoS solution, you might need to perform all of the tasks in the next sections. You will need to make decisions about these characteristics:

- Which packets are assigned (by DSCP or CoS value) to each queue?
- What drop percentage thresholds apply to each queue, and which CoS or DSCP values map to each threshold?
- How much of the available buffer space is allocated between the queues?
• How much of the available bandwidth is allocated between the queues?
• Is there traffic (such as voice) that should be given high priority?

These sections contain this configuration information:
• Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds, page 34-73 (optional)
• Allocating Buffer Space Between the Ingress Queues, page 34-74 (optional)
• Allocating Bandwidth Between the Ingress Queues, page 34-75 (optional)
• Configuring the Ingress Priority Queue, page 34-76 (optional)

Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds

You can prioritize traffic by placing packets with particular DSCPs or CoSs into certain queues and adjusting the queue thresholds so that packets with lower priorities are dropped.

Beginning in privileged EXEC mode, follow these steps to map DSCP or CoS values to an ingress queue and to set WTD thresholds. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mls qos srr-queue input dscp-map queue <strong>queue-id</strong> threshold <strong>threshold-id</strong> dscp1...dscp8</td>
</tr>
<tr>
<td></td>
<td>Map DSCP or CoS values to an ingress queue and to a threshold ID.</td>
</tr>
<tr>
<td></td>
<td>By default, DSCP values 0–39 and 48–63 are mapped to queue 1 and threshold 1. DSCP values 40–47 are mapped to queue 2 and threshold 1.</td>
</tr>
<tr>
<td></td>
<td>By default, CoS values 0–4, 6, and 7 are mapped to queue 1 and threshold 1. CoS value 5 is mapped to queue 2 and threshold 1.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>queue-id</strong>, the range is 1 to 2.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>threshold-id</strong>, the range is 1 to 3. The drop-threshold percentage for threshold 3 is predefined. It is set to the queue-full state.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>dscp1...dscp8</strong>, enter up to eight values, and separate each value with a space. The range is 0 to 63.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>cos1...cos8</strong>, enter up to eight values, and separate each value with a space. The range is 0 to 7.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>mls qos srr-queue input threshold <strong>queue-id</strong> threshold-percentage1 threshold-percentage2</td>
</tr>
<tr>
<td></td>
<td>Assign the two WTD threshold percentages for (threshold 1 and 2) to an ingress queue. The default, both thresholds are set to 100 percent.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>queue-id</strong>, the range is 1 to 2.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>threshold-percentage1 threshold-percentage2</strong>, the range is 1 to 100. Separate each value with a space.</td>
</tr>
<tr>
<td></td>
<td>Each threshold value is a percentage of the total number of queue descriptors allocated for the queue.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>


To return to the default CoS input queue threshold map or the default DSCP input queue threshold map, use the `no mls qos srr-queue input cos-map` or the `no mls qos srr-queue input dscp-map` global configuration command. To return to the default WTD threshold percentages, use the `no mls qos srr-queue input threshold queue-id` global configuration command.

This example shows how to map DSCP values 0 to 6 to ingress queue 1 and to threshold 1 with a drop threshold of 50 percent. It maps DSCP values 20 to 26 to ingress queue 1 and to threshold 2 with a drop threshold of 70 percent:

Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 1 2 3 4 5 6
Switch(config)# mls qos srr-queue input dscp-map queue 1 threshold 2 20 21 22 23 24 25 26

In this example, the DSCP values (0 to 6) are assigned the WTD threshold of 50 percent and will be dropped sooner than the DSCP values (20 to 26) assigned to the WTD threshold of 70 percent.

**Allocating Buffer Space Between the Ingress Queues**

You define the ratio (allocate the amount of space) with which to divide the ingress buffers between the two queues. The buffer and the bandwidth allocation control how much data can be buffered before packets are dropped.

Beginning in privileged EXEC mode, follow these steps to allocate the buffers between the ingress queues. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>mls qos srr-queue input buffers</code> <code>percentage1 percentage2</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>end</td>
</tr>
</tbody>
</table>
To return to the default setting, use the **no mls qos srr-queue input buffers** global configuration command.

This example shows how to allocate 60 percent of the buffer space to ingress queue 1 and 40 percent of the buffer space to ingress queue 2:

```
Switch(config)# mls qos srr-queue input buffers 60 40
```

**Allocating Bandwidth Between the Ingress Queues**

You need to specify how much of the available bandwidth is allocated between the ingress queues. The ratio of the weights is the ratio of the frequency in which the SRR scheduler sends packets from each queue. The bandwidth and the buffer allocation control how much data can be buffered before packets are dropped. On ingress queues, SRR operates only in shared mode.

Beginning in privileged EXEC mode, follow these steps to allocate bandwidth between the ingress queues. This procedure is optional.

### Command Table

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos srr-queue input bandwidth <strong>weight1</strong> <strong>weight2</strong></td>
<td>Assign shared round robin weights to the ingress queues. The default setting for <strong>weight1</strong> and <strong>weight2</strong> is 4 (1/2 of the bandwidth is equally shared between the two queues). For <strong>weight1</strong> and <strong>weight2</strong>, the range is 1 to 100. Separate each value with a space. SRR services the priority queue for its configured weight as specified by the <strong>bandwidth</strong> keyword in the <strong>mls qos srr-queue input priority-queue queue-id bandwidth weight</strong> global configuration command. Then, SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the **mls qos srr-queue input bandwidth <strong>weight1</strong> <strong>weight2</strong> global configuration command. For more information, see the “Configuring the Ingress Priority Queue” section on page 34-76.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos interface queueing</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>or</td>
<td>show mls qos input-queue</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no mls qos srr-queue input bandwidth** global configuration command.
This example shows how to assign the ingress bandwidth to the queues. Priority queueing is disabled, and the shared bandwidth ratio allocated to queue 1 is 25/(25+75) and to queue 2 is 75/(25+75):

Switch(config)# mls qos srr-queue input priority-queue 2 bandwidth 0
Switch(config)# mls qos srr-queue input bandwidth 25 75

### Configuring the Ingress Priority Queue

You should use the priority queue only for traffic that needs to be expedited (for example, voice traffic, which needs minimum delay and jitter).

The priority queue is guaranteed part of the bandwidth to reduce the delay and jitter under heavy network traffic on an oversubscribed ring (when there is more traffic than the backplane can carry, and the queues are full and dropping frames).

SRR services the priority queue for its configured weight as specified by the bandwidth keyword in the `mls qos srr-queue input priority-queue queue-id bandwidth weight` global configuration command. Then, SRR shares the remaining bandwidth with both ingress queues and services them as specified by the weights configured with the `mls qos srr-queue input bandwidth weight1 weight2` global configuration command.

Beginning in privileged EXEC mode, follow these steps to configure the priority queue. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2  | `mls qos srr-queue input priority-queue queue-id bandwidth weight` Assign a queue as the priority queue and guarantee bandwidth on the internal ring if the ring is congested. By default, the priority queue is queue 2, and 10 percent of the bandwidth is allocated to it.  
- For `queue-id`, the range is 1 to 2.  
- For `bandwidth weight`, assign the bandwidth percentage of the internal ring. The range is 0 to 40. The amount of bandwidth that can be guaranteed is restricted because a large value affects the entire ring and can degrade performance. |
| Step 3  | `end` Return to privileged EXEC mode. |
| Step 4  | `show mls qos interface queueing` or `show mls qos input-queue` Verify your entries. |
| Step 5  | `copy running-config startup-config` (Optional) Save your entries in the configuration file. |

To return to the default setting, use the `no mls qos srr-queue input priority-queue queue-id` global configuration command. To disable priority queueing, set the bandwidth weight to 0, for example, `mls qos srr-queue input priority-queue queue-id bandwidth 0`. 
This example shows how to assign the ingress bandwidths to the queues. Queue 1 is the priority queue with 10 percent of the bandwidth allocated to it. The bandwidth ratios allocated to queues 1 and 2 is 4/(4+4). SRR services queue 1 (the priority queue) first for its configured 10 percent bandwidth. Then SRR equally shares the remaining 90 percent of the bandwidth between queues 1 and 2 by allocating 45 percent to each queue:

```
Switch(config)# mls qos srr-queue input priority-queue 1 bandwidth 10
Switch(config)# mls qos srr-queue input bandwidth 4 4
```

**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 next sections. You will need to make decisions about these characteristics:

- Which packets are mapped by DSCP or CoS value to each queue and threshold ID?
- What drop percentage thresholds apply to the queue-set (four egress queues per port), and how much reserved and maximum memory is needed for the traffic type?
- How much of the fixed buffer space is allocated to the queue-set?
- Does the bandwidth of the port need to be rate limited?
- How often should the egress queues be serviced and which technique (shaped, shared, or both) should be used?

These sections contain this configuration information:

- Configuration Guidelines, page 34-77
- Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set, page 34-77 (optional)
- Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID, page 34-80 (optional)
- Configuring SRR Shaped Weights on Egress Queues, page 34-81 (optional)
- Configuring SRR Shared Weights on Egress Queues, page 34-82 (optional)
- Configuring the Egress Expedite Queue, page 34-83 (optional)
- Limiting the Bandwidth on an Egress Interface, page 34-83 (optional)

**Configuration Guidelines**

Follow these guidelines when the expedite queue is enabled or the egress queues are serviced based on their SRR weights:

- If the egress expedite queue is enabled, it overrides the SRR shaped and shared weights for queue 1.
- If the egress expedite queue is disabled and the SRR shaped and shared weights are configured, the shaped mode overrides the shared mode for queue 1, and SRR services this queue in shaped mode.
- If the egress expedite queue is disabled and the SRR shaped weights are not configured, SRR services this queue in shared mode.

**Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set**

You can guarantee the availability of buffers, set WTD thresholds, and configure the maximum allocation for a queue-set by using the `mls qos queue-set output qset-id threshold queue-id drop-threshold1 drop-threshold2 reserved-threshold maximum-threshold` global configuration commands.
Each threshold value is a percentage of the queues allocated buffers, which you specify by using the `mls qos queue-set output qset-id buffers allocation1 ... allocation4` global configuration command. The queues use WTD to support distinct drop percentages for different traffic classes.

**Note**
The egress queue default settings are suitable for most situations. You should change them only when you have a thorough understanding of the egress queues and if these settings do not meet your QoS solution.

Beginning in privileged EXEC mode, follow these steps to configure the memory allocation and to drop thresholds for a queue-set. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</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>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `mls qos queue-set output qset-id buffers allocation1 ... allocation4` | Allocate buffers to a queue-set. By default, all allocation values are equally mapped among the four queues (25, 25, 25, 25). Each queue has 1/4 of the buffer space.  
  • For `qset-id`, enter the ID of the queue-set. The range is 1 to 2. Each port belongs to a queue-set, which defines all the characteristics of the four egress queues per port.  
  • For `allocation1 ... allocation4`, specify four percentages, one for each queue in the queue-set. For `allocation1, allocation3, and allocation4`, the range is 0 to 99. For `allocation2`, the range is 1 to 100 (including the CPU buffer).  
  Allocate buffers according to the importance of the traffic; for example, give a large percentage of the buffer to the queue with the best-effort traffic. |
### Step 3

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mls qos queue-set output</code> <em>qset-id</em> <code>threshold</code> <em>queue-id</em> <code>drop-threshold1</code> <code>drop-threshold2</code> <code>reserved-threshold</code> <code>maximum-threshold</code></td>
<td>Configure the WTD thresholds, guarantee the availability of buffers, and configure the maximum memory allocation for the queue-set (four egress queues per port). By default, the WTD thresholds for queues 1, 3, and 4 are set to 100 percent. The thresholds for queue 2 are set to 200 percent. The reserved thresholds for queues 1, 2, 3, and 4 are set to 50 percent. The maximum thresholds for all queues are set to 400 percent.</td>
</tr>
</tbody>
</table>

- For `qset-id`, enter the ID of the queue-set specified in Step 2. The range is 1 to 2.
- For `queue-id`, enter the specific queue in the queue-set on which the command is performed. The range is 1 to 4.
- For `drop-threshold1` `drop-threshold2`, specify the two WTD thresholds expressed as a percentage of the queue’s allocated memory. The range is 1 to 3200 percent.
- For `reserved-threshold`, enter the amount of memory to be guaranteed (reserved) for the queue expressed as a percentage of the allocated memory. The range is 1 to 100 percent.
- For `maximum-threshold`, enable a queue in the full condition to obtain more buffers than are reserved for it. This is the maximum memory the queue can have before the packets are dropped if the common pool is not empty. The range is 1 to 3200 percent. |

### Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code> <em>interface-id</em></td>
<td>Specify the port of the outbound traffic, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>

### Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>queue</code> <em>qset-id</em></td>
<td>Map the port to a queue-set. For <code>qset-id</code>, enter the ID of the queue-set specified in Step 2. The range is 1 to 2. The default is 1.</td>
</tr>
</tbody>
</table>

### Step 6

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

### Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mls qos interface</code> <code>[interface-id]</code> <code>buffers</code></td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

### Step 8

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no mls qos queue-set output qset-id buffers` global configuration command. To return to the default WTD threshold percentages, use the `no mls qos queue-set output qset-id threshold` `[queue-id]` global configuration command.

This example shows how to map a port to queue-set 2. It allocates 40 percent of the buffer space to egress queue 1 and 20 percent to egress queues 2, 3, and 4. It configures the drop thresholds for queue 2 to 40 and 60 percent of the allocated memory, guarantees (reserves) 100 percent of the allocated memory, and configures 200 percent as the maximum memory that this queue can have before packets are dropped:

```
Switch(config)# mls qos queue-set output 2 buffers 40 20 20 20
Switch(config)# mls qos queue-set output 2 threshold 2 40 60 100 200
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# queue-set 2
```
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.

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 map DSCP or CoS values to an egress queue and to a threshold ID. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mls qos srr-queue output dscp-map queue queue-id threshold threshold-id dscp1...dscp8</td>
</tr>
<tr>
<td>or</td>
<td>mls qos srr-queue output cos-map queue queue-id threshold threshold-id cos1...cos8</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show mls qos maps</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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.
This example shows how to map DSCP values 10 and 11 to egress queue 1 and to threshold 2:

```
Switch(config)# mls qos srr-queue output dscp-map queue 1 threshold 2 10 11
```

**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. For information about shaped weights, see the “SRR Shaping and Sharing” section on page 34-15. For information about shared weights, see the “Configuring SRR Shared Weights on Egress Queues” section on page 34-82.

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.

<table>
<thead>
<tr>
<th>Command</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>Step 2</strong> interface interface-id</td>
<td>Specifying the port of the outbound traffic, and enter interface config</td>
</tr>
<tr>
<td><strong>Step 3</strong> srr-queue bandwidth shape weight1</td>
<td>Assigning SRR weights to the egress queues.</td>
</tr>
<tr>
<td>weight2 weight3 weight4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> show mls qos interface interface-id queueing</td>
<td>Verifying your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong> copy running-config startup-config</td>
<td>(Optional) Saving your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no srr-queue bandwidth shape` interface configuration command.

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 gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth shape 8 0 0 0
```
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port of the outbound traffic, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 srr-queue bandwidth share weight1 weight2 weight3 weight4</td>
<td>Assign SRR weights to the egress queues.</td>
</tr>
<tr>
<td></td>
<td>By default, all four weights are 25 (1/4 of the bandwidth is allocated to each queue).</td>
</tr>
<tr>
<td></td>
<td>For weight1 weight2 weight3 weight4, 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.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show mls qos interface interface-id queueing</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no srr-queue bandwidth share interface configuration command.

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 gigabitethernet0/1
Switch(config-if)# srr-queue bandwidth share 1 2 3 4
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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mls qos</td>
<td>Enable QoS on a switch.</td>
</tr>
<tr>
<td>Step 3 interface interface-id</td>
<td>Specify the egress port, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 priority-queue out</td>
<td>Enable the egress expedite queue, which is disabled by default.</td>
</tr>
<tr>
<td></td>
<td>When you configure this command, the SRR weight and queue size ratios are affected because there is one less 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).</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the egress expedite queue, use the no priority-queue out interface configuration command.

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 gigabitethernet0/1
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
```

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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to be rate limited, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
To return to the default setting, use the `no srr-queue bandwidth limit` interface configuration command.

This example shows how to limit the bandwidth on a port to 80 percent:

```
Switch(config)# interface gigabitethernet0/1
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.

### Displaying Standard QoS Information

To display standard QoS information, use one or more of the privileged EXEC commands in Table 34-15:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show class-map [class-map-name]</code></td>
<td>Display QoS class maps, which define the match criteria to classify traffic.</td>
</tr>
<tr>
<td><code>show mls qos</code></td>
<td>Display global QoS configuration information.</td>
</tr>
<tr>
<td><code>show mls qos aggregate-policer [aggregate-policer-name]</code></td>
<td>Display the aggregate policer configuration.</td>
</tr>
<tr>
<td><code>show mls qos input-queue</code></td>
<td>Display QoS settings for the ingress queues.</td>
</tr>
<tr>
<td>`show mls qos interface [interface-id] [buffers</td>
<td>policers</td>
</tr>
<tr>
<td><code>show mls qos queue-set [qset-id]</code></td>
<td>Display QoS settings for the egress queues.</td>
</tr>
<tr>
<td><code>show mls qos vlan vlan-id</code></td>
<td>Display the policy maps attached to the specified SVI.</td>
</tr>
</tbody>
</table>
Displaying Standard QoS Information

### Table 34-15  Commands for Displaying Standard QoS Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `show policy-map [policy-map-name [class class-map-name]]` | Display QoS policy maps, which define classification criteria for incoming traffic.  
**Note**  
Do not use the `show policy-map interface` privileged EXEC command to display classification information for incoming traffic. The `control-plane` and `interface` keywords are not supported, and the statistics shown in the display should be ignored. |
| `show running-config | include rewrite` | Display the DSCP transparency setting. |
CHAPTER 35

Configuring EtherChannels and Link-State Tracking

This chapter describes how to configure EtherChannels on the Catalyst 3560 switch. EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use it 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. This chapter also describes how to configure link-state tracking.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release.

- Understanding EtherChannels, page 35-2
- Configuring EtherChannels, page 35-9
- Displaying EtherChannel, PAgP, and LACP Status, page 35-20
- Understanding Link-State Tracking, page 35-21
- Configuring Link-State Tracking, page 35-23
Understanding EtherChannels

- EtherChannel Overview, page 35-2
- Port-Channel Interfaces, page 35-3
- Port Aggregation Protocol, page 35-4
- Link Aggregation Control Protocol, page 35-6
- EtherChannel On Mode, page 35-7
- Load Balancing and Forwarding Methods, page 35-7

EtherChannel Overview

An EtherChannel consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link as shown in Figure 35-1.

![Figure 35-1 Typical EtherChannel Configuration](image)

The EtherChannel provides full-duplex bandwidth up to 800 Mb/s (Fast EtherChannel) or 8 Gb/s (Gigabit EtherChannel) between your switch and another switch or host. Each EtherChannel can consist of up to eight compatibly configured Ethernet ports.
All ports in each EtherChannel must be configured as either Layer 2 or Layer 3 ports. The number of EtherChannels is limited to 48. The EtherChannel Layer 3 ports are made up of routed ports. Routed ports are physical ports configured to be in Layer 3 mode by using the `no switchport` interface configuration command. For more information, see the Chapter 11, “Configuring Interface Characteristics.”

For more information, see the “EtherChannel Configuration Guidelines” section on page 35-10.

You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or On. Configure both ends of the EtherChannel in the same mode:

- When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. Incompatible ports are put into an independent state and continue to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

- When you configure an EtherChannel in the `on` mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the `on` mode; otherwise, packet loss can occur.

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

### Port-Channel Interfaces

When you create an EtherChannel, a port-channel logical interface is involved:

- With Layer 2 ports, use the `channel-group` interface configuration command to dynamically create the port-channel logical interface.

You also can use the `interface port-channel port-channel-number` global configuration command to manually create the port-channel logical 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.

- With Layer 3 ports, you should manually create the logical interface by using the `interface port-channel` global configuration command followed by the `no switchport` interface configuration command. Then you manually assign an interface to the EtherChannel by using the `channel-group` interface configuration command.

For both Layer 2 and Layer 3 ports, the `channel-group` command binds the physical port and the logical interface together as shown in Figure 35-2.

Each EtherChannel has a port-channel logical interface numbered from 1 to 48. This port-channel interface number corresponds to the one specified with the `channel-group` interface configuration command.
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. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

**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 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

Table 35-1 shows the user-configurable EtherChannel PAgP modes for the channel-group interface configuration command.

<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, trunking 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 desirable mode because neither port starts PAgP negotiation.

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.

PAgP Interaction with Virtual Switches and Dual-Active Detection

A virtual switch can be two or more Catalyst 6500 core switches connected by virtual switch links (VSLs) that carry control and data traffic between them. One of the switches is in active mode. The others are in standby mode. For redundancy, remote switches, such as Catalyst 3650 switches, are connected to the virtual switch by remote satellite links (RSLs).

If the VSL between two switches fails, one switch does not know the status of the other. Both switches could change to the active mode, causing a dual-active situation in the network with duplicate configurations (including duplicate IP addresses and bridge identifiers). The network might go down.
To prevent a dual-active situation, the core switches send PAgP protocol data units (PDUs) through the RSLs to the remote switches. The PAgP PDUs identify the active switch, and the remote switches forward the PDUs to core switches so that the core switches are in sync. If the active switch fails or resets, the standby switch takes over as the active switch. If the VSL goes down, one core switch knows the status of the other and does not change state.

**PAgP Interaction with Other Features**

The Dynamic Trunking Protocol (DTP) and the Cisco Discovery Protocol (CDP) send and receive packets over the physical ports in the EtherChannel. Trunk ports send and receive PAgP protocol data units (PDUs) on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

PAgP sends and receives PAgP PDUs only from ports that are up and have PAgP enabled for the auto or desirable mode.

**Link Aggregation Control Protocol**

The LACP is defined in IEEE 802.3ad and enables Cisco switches to manage Ethernet channels between switches that conform to the IEEE 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

By using LACP, the switch learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single switch port.

**LACP Modes**

Table 35-2 shows the user-configurable EtherChannel LACP modes for the `channel-group` interface configuration command.

<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, trunking 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.

**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.

**Load Balancing and Forwarding Methods**

EtherChannel balances the traffic load across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The selected mode applies to all EtherChannels configured on the switch. You configure the load balancing and forwarding method by using the **port-channel load-balance** global configuration command.

With source-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source-MAC address of the incoming packet. Therefore, to provide load balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel.
With destination-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the destination host’s MAC address of the incoming packet. Therefore, packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

With source-and-destination MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on both the source and destination MAC addresses. This forwarding method, a combination source-MAC and destination-MAC address forwarding methods of load distribution, can be used if it is not clear whether source-MAC or destination-MAC address forwarding is better suited on a particular switch. With source-and-destination MAC-address forwarding, packets sent from host A to host B, host A to host C, and host C to host B could all use different ports in the channel.

With source-IP address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the source-IP address of the incoming packet. Therefore, to provide load-balancing, packets from different IP addresses use different ports in the channel, but packets from the same IP address use the same port in the channel.

With destination-IP address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the destination-IP address of the incoming packet. Therefore, to provide load-balancing, packets from the same IP source address sent to different IP destination addresses could be sent on different ports in the channel. But packets sent from different source IP addresses to the same destination IP address are always sent on the same port in the channel.

With source-and-destination IP address-based forwarding, packets are sent to an EtherChannel and distributed across the EtherChannel ports, based on both the source and destination IP addresses of the incoming packet. This forwarding method, a combination of source-IP and destination-IP address-based forwarding, can be used if it is not clear whether source-IP or destination-IP address-based forwarding is better suited on a particular switch. In this method, packets sent from the IP address A to IP address B, from IP address A to IP address C, and from IP address C to IP address B could all use different ports in the channel.

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch in the network and the kind of traffic that needs to be load-distributed. In Figure 35-3, an EtherChannel from a switch that is aggregating data from four workstations communicates with a router. Because the router is a single-MAC-address device, source-based forwarding on the switch EtherChannel ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of workstations ensures that the traffic is evenly distributed from the router EtherChannel.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is only going to a single MAC address, using the destination-MAC address always chooses the same link in the channel. Using source addresses or IP addresses might result in better load balancing.
Configuring EtherChannels

These sections contain this configuration information:

- Default EtherChannel Configuration, page 35-10
- EtherChannel Configuration Guidelines, page 35-10
- Configuring Layer 2 EtherChannels, page 35-11 (required)
- Configuring Layer 3 EtherChannels, page 35-13 (required)
- Configuring EtherChannel Load Balancing, page 35-16 (optional)
- Configuring the PAgP Learn Method and Priority, page 35-17 (optional)
- Configuring LACP Hot-Standby Ports, page 35-18 (optional)

**Note**

Make sure that the ports are correctly configured. For more information, see the “EtherChannel Configuration Guidelines” section on page 35-10.

**Note**

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.
Default EtherChannel Configuration

Table 35-3 shows the default EtherChannel configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel groups</td>
<td>None assigned.</td>
</tr>
<tr>
<td>Port-channel logical interface</td>
<td>None defined.</td>
</tr>
<tr>
<td>PAgP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>PAgP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>PAgP priority</td>
<td>128 on all ports.</td>
</tr>
<tr>
<td>LACP mode</td>
<td>No default.</td>
</tr>
<tr>
<td>LACP learn method</td>
<td>Aggregate-port learning on all ports.</td>
</tr>
<tr>
<td>LACP port priority</td>
<td>32768 on all ports.</td>
</tr>
<tr>
<td>LACP system priority</td>
<td>32768.</td>
</tr>
<tr>
<td>LACP system ID</td>
<td>LACP system priority and the switch MAC address.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>Load distribution on the switch is based on the source-MAC address of the incoming packet.</td>
</tr>
</tbody>
</table>

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:

- Do not try to configure more than 48 EtherChannels on the switch.
- 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 Switched Port Analyzer (SPAN) destination port as part of an EtherChannel.

Do not configure a secure port as part of an EtherChannel or the reverse.

Do not configure a private-VLAN port as part of an EtherChannel.

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.

For Layer 2 EtherChannels:

- Assign all ports in the EtherChannel to the same VLAN, or configure them as trunks. Ports with different native VLANs cannot form an EtherChannel.
- If you configure an EtherChannel from trunk ports, verify that the trunking mode (ISL or IEEE 802.1Q) is the same on all the trunks. Inconsistent trunk modes on EtherChannel ports can have unexpected results.
- 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.

For Layer 3 EtherChannels, assign the Layer 3 address to the port-channel logical interface, not to the physical ports in the channel.

### 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.
Beginning in privileged EXEC mode, follow these steps to assign a Layer 2 Ethernet port to a Layer 2 EtherChannel. This procedure is required.

<table>
<thead>
<tr>
<th>Command</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> interface interface-id</td>
<td>Specify a physical port, and enter interface configuration mode. Valid interfaces include physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> switchport mode {access</td>
<td>Assign all ports as static-access ports in the same VLAN, or configure them as trunks. If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td>trunk} switchport access vlan vlan-id</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> channel-group channel-group-number mode {auto [non-silent]</td>
<td>Assign the port to a channel group, and specify the PAgP or the LACP mode. For channel-group-number, the range is 1 to 48. For mode, select one of these keywords:</td>
</tr>
<tr>
<td>[desirable [non-silent]</td>
<td>mode}</td>
</tr>
<tr>
<td>on}</td>
<td>• auto—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.</td>
</tr>
<tr>
<td></td>
<td>• desirable—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.</td>
</tr>
<tr>
<td></td>
<td>• on—Forces the port to channel without PAgP or LACP. In the on mode, an EtherChannel exists only when a port group in the on mode is connected to another port group in the on mode.</td>
</tr>
<tr>
<td></td>
<td>• non-silent—(Optional) If your switch is connected to a partner that is PAgP-capable, configure the switch port for nonsilent operation when the port is in the auto or desirable mode. If you do not specify non-silent, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.</td>
</tr>
<tr>
<td></td>
<td>• active—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.</td>
</tr>
<tr>
<td></td>
<td>• passive—Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
To remove a port from the EtherChannel group, use the `no channel-group` interface configuration command.

This example shows how to configure an EtherChannel on a switch. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the PAgP mode `desirable`:

```plaintext
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 switch. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the LACP mode `active`:

```plaintext
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
```

## Configuring Layer 3 EtherChannels

To configure Layer 3 EtherChannels, you create the port-channel logical interface and then put the Ethernet ports into the port-channel as described in the next two sections.

### Creating Port-Channel Logical Interfaces

When configuring Layer 3 EtherChannels, you should first manually create the port-channel logical interface by using the `interface port-channel` global configuration command. Then you put the logical interface into the channel group by using the `channel-group` interface configuration command.

**Note**
To move an IP address from a physical port to an EtherChannel, you must delete the IP address from the physical port before configuring it on the port-channel interface.

Beginning in privileged EXEC mode, follow these steps to create a port-channel interface for a Layer 3 EtherChannel. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface port-channel port-channel-number</code></td>
<td>Specify the port-channel logical interface, and enter interface configuration mode. For <code>port-channel-number</code>, the range is 1 to 48.</td>
</tr>
</tbody>
</table>
Chapter 35 Configuring EtherChannels and Link-State Tracking

Configuring EtherChannels

To remove the port-channel, use the `no interface port-channel port-channel-number` global configuration command.

This example shows how to create the logical port channel 5 and assign 172.10.20.10 as its IP address:

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

Configuring the Physical Interfaces

Beginning in privileged EXEC mode, follow these steps to assign an Ethernet port to a Layer 3 EtherChannel. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Specify a physical port, and enter interface configuration mode. Valid interfaces include physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>no ip address</code> Ensure that there is no IP address assigned to the physical port.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>no switchport</code> Put the port into Layer 3 mode.</td>
</tr>
</tbody>
</table>
Chapter 35  Configuring EtherChannels and Link-State Tracking

Configuring EtherChannels

Step 5

channel-group channel-group-number mode
{auto [non-silent] | desirable [non-silent] | on} |
{active | passive}

Assign the port to a channel group, and specify the PAgP or the LACP mode.

For channel-group-number, the range is 1 to 48. This number must be the same as the port-channel-number (logical port) configured in the “Creating Port-Channel Logical Interfaces” section on page 35-13.

For mode, select one of these keywords:

- **auto**—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.

- **desirable**—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.

- **on**—Forces the port to channel without PAgP or LACP. In the on mode, an EtherChannel exists only when a port group in the on mode is connected to another port group in the on mode.

- **non-silent**—(Optional) If your switch is connected to a partner that is PAgP capable, configure the switch port for nonsilent operation when the port is in the auto or desirable mode. If you do not specify non-silent, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.

- **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.

- **passive**—Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.

For information on compatible modes for the switch and its partner, see the “PAgP Modes” section on page 35-5 and the “LACP Modes” section on page 35-6.

Step 6

end

Return to privileged EXEC mode.

Step 7

show running-config

Verify your entries.

Step 8

copy running-config startup-config

(Optional) Save your entries in the configuration file.
### Configuring EtherChannels

This example shows how to configure an EtherChannel. It assigns two ports to channel 5 with the LACP mode active:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

#### Configuring EtherChannel Load Balancing

This section describes how to configure EtherChannel load balancing by using source-based or destination-based forwarding methods. For more information, see the “Load Balancing and Forwarding Methods” section on page 35-7.

Beginning in privileged EXEC mode, follow these steps to configure EtherChannel load balancing. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>port-channel load-balance {dst-ip</td>
</tr>
<tr>
<td></td>
<td>Configure an EtherChannel load-balancing method. The default is src-mac.</td>
</tr>
<tr>
<td></td>
<td>Select one of these load-distribution methods:</td>
</tr>
<tr>
<td></td>
<td>- dst-ip—Load distribution is based on the destination-host IP address.</td>
</tr>
<tr>
<td></td>
<td>- dst-mac—Load distribution is based on the destination-host MAC address of the incoming packet.</td>
</tr>
<tr>
<td></td>
<td>- src-dst-ip—Load distribution is based on the source-and-destination host-IP address.</td>
</tr>
<tr>
<td></td>
<td>- src-dst-mac—Load distribution is based on the source-and-destination host-MAC address.</td>
</tr>
<tr>
<td></td>
<td>- src-ip—Load distribution is based on the source-host IP address.</td>
</tr>
<tr>
<td></td>
<td>- src-mac—Load distribution is based on the source-MAC address of the incoming packet.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show etherchannel load-balance</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return EtherChannel load balancing to the default configuration, use the no port-channel load-balance global configuration command.
Configuring the PAgP Learn Method and Priority

Network devices are classified as PAgP physical learners or aggregate-port learners. A device is a physical learner if it learns addresses by physical ports and directs transmissions based on that knowledge. A device is an aggregate-port learner if it learns addresses by aggregate (logical) ports. The learn method must be configured the same at both ends of the link.

When a device and its partner are both aggregate-port learners, they learn the address on the logical port-channel. The device sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives.

PAgP cannot automatically detect when the partner device is a physical learner and when the local device is an aggregate-port learner. Therefore, you must manually set the learning method on the local device to learn addresses by physical ports. You also must set the load-distribution method to source-based distribution, so that any given source MAC address is always sent on the same physical port.

You also can configure a single port within the group for all transmissions and use other ports for hot standby. The unused ports in the group can be swapped into operation in just a few seconds if the selected single port loses hardware-signal detection. You can configure which port is always selected for packet transmission by changing its priority with the `pagp port-priority` interface configuration command. The higher the priority, the more likely that the port will be selected.

Note

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.

When the link partner of the switch is a physical learner (such as a Catalyst 1900 series switch), we recommend that you configure the Catalyst 3560 switch as a physical-port learner by using the `pagp learn-method physical-port` interface configuration command. Set the load-distribution method based on the source MAC address by using the `port-channel load-balance src-mac` global configuration command. The switch then sends packets to the Catalyst 1900 switch using the same port in the EtherChannel from which it learned the source address. Only use the `pagp learn-method` command in this situation.

Beginning in privileged EXEC mode, follow these steps to configure your switch as a PAgP physical-port learner and to adjust the priority so that the same port in the bundle is selected for sending packets. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specify the port for transmission, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring EtherChannels

#### Configuring EtherChannels

**To return the priority to its default setting,** use the `no pagp port-priority` interface configuration command.

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.

Select **physical-port** to connect with another switch that is a physical learner. Make sure to configure the `port-channel load-balance` global configuration command to `src-mac` as described in the “Configuring EtherChannel Load Balancing” section on page 35-16.

The learning method must be configured the same at both ends of the link.

**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. For more information, see the “Configuring the LACP System Priority” section on page 35-19 and the “Configuring the LACP Port Priority” section on page 35-19.

**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).

Beginning in privileged EXEC mode, follow these steps to configure the LACP system priority. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2 | `lacp system-priority priority` | Configure the LACP system priority.  
For `priority`, the range is 1 to 65535. The default is 32768.  
The lower the value, the higher the system priority. |
| Step 3 | `end` | Return to privileged EXEC mode. |
| Step 4 | `show running-config`  
or  
`show lacp sys-id` | Verify your entries. |
| Step 5 | `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

To return the LACP system priority to the default value, use the `no lacp system-priority` global configuration command.

**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.

Beginning in privileged EXEC mode, follow these steps to configure the LACP port priority. This procedure is optional.

**Command** | **Purpose**
--- | ---
Step 1 | configure terminal
Enter global configuration mode.
Step 2 | interface interface-id
Specify the port to be configured, and enter interface configuration mode.
Step 3 | lacp port-priority priority
Configure the LACP port priority. 
For priority, the range is 1 to 65535. The default is 32768. The lower the value, the more likely that the port will be used for LACP transmission.
Step 4 | end
Return to privileged EXEC mode.
Step 5 | show running-config
or
show lacp [channel-group-number] internal
Verify your entries.
Step 6 | copy running-config startup-config
(Optional) Save your entries in the configuration file.

To return the LACP port priority to the default value, use the no lacp port-priority interface configuration command.

## Displaying EtherChannel, PAgP, and LACP Status

### Table 35-4 Commands for Displaying EtherChannel, PAgP, and LACP Status

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show etherchannel [channel-group-number] {detail</td>
<td>port</td>
</tr>
<tr>
<td>show pagp [channel-group-number] {counters</td>
<td>internal</td>
</tr>
<tr>
<td>show pagp [channel-group-number] dual-active</td>
<td>Displays the dual-active detection status.</td>
</tr>
<tr>
<td>show lacp [channel-group-number] {counters</td>
<td>internal</td>
</tr>
</tbody>
</table>

You can clear PAgP channel-group information and traffic counters by using the clear pagp {channel-group-number counters | counters} privileged EXEC command.
You can clear LACP channel-group information and traffic counters by using the **clear lacp**
{channel-group-number counters | counters} privileged EXEC command.

For detailed information about the fields in the displays, see the command reference for this release.

**Understanding Link-State Tracking**

Link-state tracking, also known as trunk failover, is a feature that binds the link state of multiple interfaces. For example, link-state tracking provides redundancy in the network when used with server NIC adapter teaming. When the server network adapters are configured in a primary or secondary relationship known as teaming, if the link is lost on the primary interface, connectivity is transparently changed to the secondary interface.

![Note]

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

Figure 35-4 on page 35-23 shows a network configured with link-state tracking. To enable link-state tracking, create a *link-state group*, and specify the interfaces that are assigned to the link-state group. In a link-state group, these interfaces are bundled together. The *downstream interfaces* are bound to the *upstream interfaces*. Interfaces connected to servers are referred to as downstream interfaces, and interfaces connected to distribution switches and network devices are referred to as upstream interfaces.

The configuration in Figure 35-4 ensures that the network traffic flow is balanced as follows:

- 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.
Understanding Link-State Tracking

- 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.

As an example of a connectivity change from link-state group 1 to link-state group 2 on switch A, see Figure 35-4 on page 35-23. 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.
Figure 35-4 Typical Link-State Tracking Configuration

Configuring Link-State Tracking

- Default Link-State Tracking Configuration, page 35-23
- Link-State Tracking Configuration Guidelines, page 35-24
- Configuring Link-State Tracking, page 35-24
- Displaying Link-State Tracking Status, page 35-25

Default Link-State Tracking Configuration

There are no link-state groups defined, and link-state tracking is not enabled for any group.
Link-State Tracking Configuration Guidelines

Follow these guidelines to avoid configuration problems:

- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.
- Do not enable link-state tracking on individual interfaces that will be part of a downstream Etherchannel interface.
- An interface cannot be a member of more than one link-state group.
- You can configure only two link-state groups per switch.

Configuring Link-State Tracking

Beginning in privileged EXEC mode, follow these steps to configure a link-state group and to assign an interface to a group:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>link state track number</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>link state group [number] {upstream</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to create a link-state group and configure the interfaces:
```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# 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
```
To disable a link-state group, use the `no link state track number` global configuration command.

**Displaying Link-State Tracking Status**

Use the `show link state group` command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group. Enter the detail keyword to display detailed information about the group.

This is an example of output from the `show link state group` command:

```
Switch> show link state group 1
Link State Group: 1      Status: Enabled, Down
```

This is an example of output from the `show link state group detail` command:

```
Switch> show link state group detail
(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled
Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Gi0/15(Dwn) Gi0/16(Dwn)
Downstream Interfaces : Gi0/11(Dis) Gi0/12(Dis) Gi0/13(Dis) Gi0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Gi1/0/15(Dwn) Gi1/0/16(Dwn) Gi1/0/17(Dwn)
Downstream Interfaces : Gi1/0/11(Dis) Gi1/0/12(Dis) Gi1/0/13(Dis) Gi1/0/14(Dis)
(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

For detailed information about the fields in the display, see the command reference for this release.
Configuring TelePresence E911 IP Phone Support

Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack.
The Catalyst 3560 switch command reference has command syntax and usage information.
- Understanding TelePresence E911 IP Phone Support, page 36-1
- Configuring TelePresence E911 IP Phone Support, page 36-2

Understanding TelePresence E911 IP Phone Support

You can use a Cisco IP phone as a user interface in a Cisco TelePresence System. See in Figure 1. In this configuration, the IP phone must always be on and available for emergency calls. If the power to the codec in the Cisco TelePresence System fails, is disrupted or if the codec fails, the IP phone is not available.

Figure 36-1 Phone-Codec-Switch Connection

1 Switch
2 Cisco TelePresence System with a codec
3 IP phone

Use the TelePresence E911 IP phone support feature to ensure that the IP phone is always on and available for emergency calls. When a CDP-enabled IP phone is connected to the codec through a switch, you can configure the switch to forward CDP packets from the IP phone only to the codec in the Cisco
TelePresence System. The switch adds *ingress-egress port pairs* to the CDP forwarding table. An ingress-egress port pair is a one-to-one mapping between an ingress switch port connected to the IP phone and an egress switch port connected to the codec.

The IP phone and the codec communicate through the IP network. If power to the codec fails, is disrupted or if the codec fails, the IP phone is still connected to the IP network and is available for emergency calls.

The switch forwards all CDP packets received on the ingress port to the egress port. If multiple IP phones are connected to the codec through a single port on the switch, only one phone communicates with it through the IP network. This phone is usually the one that sent the first CDP packet received by the codec.

**Figure 36-2  Phone-Switch-Codec Connection**

![Diagram](image)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Switch</td>
</tr>
<tr>
<td>2</td>
<td>Cisco TelePresence System with a codec</td>
</tr>
<tr>
<td>3</td>
<td>CDP-enabled IP phone</td>
</tr>
</tbody>
</table>

### Configuring TelePresence E911 IP Phone Support

- **Configuration Guidelines, page 36-2**
- **Enabling TelePresence E911 IP Phone Support, page 36-3**
- **Example, page 36-3**

### Configuration Guidelines

- You must use only CDP-enabled phones with TelePresence E911 IP phone support.
- You can connect the IP phone and codec in the Cisco TelePresence System through any two ports in a switch stack.
## Enabling TelePresence E911 IP Phone Support

Beginning in privileged EXEC mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>cdp forward ingress port-id egress port-id</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>show cdp forward</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>copy running-config startup config</code></td>
</tr>
</tbody>
</table>

### Example

```plaintext
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# cdp forward ingress gigabitethernet2/0/1 egress gigabitethernet0/12
Switch(config)# cdp forward ingress gigabitethernet2/0/1 egress gigabitethernet0/13
Ingress interface already configured
Switch(config)# cdp forward ingress gigabitethernet2/0/2 egress gigabitethernet0/12
Egress interface already configured
Switch(config)# cdp forward ingress gigabitethernet2/0/2 egress gigabitethernet0/13
Switch(config)# end
Switch# *Mar 1 13:38:34.954: %SYS-5-CONFIG_I: Configured from console by console
Switch# show running-config | include cdp
cdp forward ingress GigabitEthernet0/1 egress GigabitEthernet0/12
cdp forward ingress GigabitEthernet0/2 egress GigabitEthernet0/13
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no cdp forward ingress gigabitethernet0/1
Switch(config)# end
Switch# *Mar 1 13:39:14.120: %SYS-5-CONFIG_I: Configured from console by console
Switch# show running-config | include cdp
cdp forward ingress GigabitEthernet2/0/2 egress GigabitEthernet0/13
```

Switch# `show cdp forward`

<table>
<thead>
<tr>
<th>Ingress Port</th>
<th>Egress Port</th>
<th># packets forwarded</th>
<th># packets dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/2</td>
<td>Gi0/13</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Switch#
CHAPTER

37

Configuring IP Unicast Routing

This chapter describes how to configure IP Version 4 (IPv4) unicast routing on the Catalyst 3560 switch. Basic routing functions, including static routing and the Routing Information Protocol (RIP), are available with both the IP base image and the IP services image. To use advanced routing features and other routing protocols, you must have the IP services image installed on the switch.

Note
If the switch is running the IP services image, you can also enable IP Version 6 (IPv6) unicast routing and configure interfaces to forward IPv6 traffic in addition to IPv4 traffic. For information about configuring IPv6 on the switch, see Chapter 38, “Configuring IPv6 Unicast Routing.”

For more detailed IP unicast configuration information, see the Cisco IOS IP Configuration Guide, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides. For complete syntax and usage information for the commands used in this chapter, see these command references from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References:

- Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2
- Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2

This chapter consists of these sections:

- Understanding IP Routing, page 37-2
- Steps for Configuring Routing, page 37-3
- Configuring IP Addressing, page 37-4
- Enabling IP Unicast Routing, page 37-18
- Configuring RIP, page 37-18
- Configuring OSPF, page 37-24
- Configuring EIGRP, page 37-33
- Configuring BGP, page 37-41
- Configuring ISO CLNS Routing, page 37-62
- Configuring Multi-VRF CE, page 37-72
- Configuring Protocol-Independent Features, page 37-87
- Monitoring and Maintaining the IP Network, page 37-103
Understanding 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 37-1 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 three different ways:

- By using default routing
- By using preprogrammed static routes for the traffic
- By dynamically calculating routes by using a routing protocol

Default routing refers to sending traffic with a destination unknown to the router to a default outlet or destination.
Static unicast routing forwards packets from predetermined ports through a single path into and out of a network. Static routing is secure and uses little bandwidth, but does not automatically respond to changes in the network, such as link failures, and therefore, might result in unreachable destinations. As networks grow, static routing becomes a labor-intensive liability.

Dynamic routing protocols are used by routers to dynamically calculate the best route for forwarding traffic. There are two types of dynamic routing protocols:

- Routers using distance-vector protocols maintain routing tables with distance values of networked resources, and periodically pass these tables to their neighbors. Distance-vector protocols use one or a series of metrics for calculating the best routes. These protocols are easy to configure and use.

- Routers using link-state protocols maintain a complex database of network topology, based on the exchange of link-state advertisements (LSAs) between routers. LSAs are triggered by an event in the network, which speeds up the convergence time or time required to respond to these changes. Link-state protocols respond quickly to topology changes, but require greater bandwidth and more resources than distance-vector protocols.

Distance-vector protocols supported by the switch are Routing Information Protocol (RIP), which uses a single distance metric (cost) to determine the best path and Border Gateway Protocol (BGP), which adds a path vector mechanism. The switch also supports the Open Shortest Path First (OSPF) link-state protocol and Enhanced IGRP (EIGRP), which adds some link-state routing features to traditional Interior Gateway Routing Protocol (IGRP) to improve efficiency.

**Steps for Configuring Routing**

By default, IP routing is disabled on the switch, and you must enable it before routing can take place. 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 > 12.2 Mainline > Configuration Guides.

In the following procedures, the specified interface must be one of these Layer 3 interfaces:

- A routed port: a physical port configured as a Layer 3 port by using the `no switchport` interface configuration command.

- A switch virtual interface (SVI): a VLAN interface created by using the `interface vlan vlan_id` global configuration command and by default a Layer 3 interface.

- An EtherChannel port channel in Layer 3 mode: a port-channel logical interface created by using the `interface port-channel port-channel-number` global configuration command and binding the Ethernet interface into the channel group. For more information, see the “Configuring Layer 3 EtherChannels” section on page 35-13.

**Note**
The switch does not support tunnel interfaces for unicast routed traffic.

All Layer 3 interfaces on which routing will occur must have IP addresses assigned to them. See the “Assigning IP Addresses to Network Interfaces” section on page 37-5.
A Layer 3 switch can have an IP address assigned to each routed port and SVI. The number of routed ports and SVIs that you can configure is not limited by software. However, the interrelationship between this number and the number and volume of features being implemented might have an impact on CPU utilization because of hardware limitations. To optimize system memory for routing, use the `sdm prefer routing` global configuration command.

Configuring routing consists of several main procedures:
- To support VLAN interfaces, create and configure VLANs on the switch, and assign VLAN membership to Layer 2 interfaces. For more information, see Chapter 13, “Configuring VLANs.”
- Configure Layer 3 interfaces.
- Enable IP routing on the switch.
- Assign IP addresses to the Layer 3 interfaces.
- Enable selected routing protocols on the switch.
- Configure routing protocol parameters (optional).

### Configuring IP Addressing

A required task for configuring IP routing is to assign IP addresses to Layer 3 network interfaces to enable the interfaces and allow communication with the hosts on those interfaces that use IP. These sections describe how to configure various IP addressing features. Assigning IP addresses to the interface is required; the other procedures are optional.

- Default Addressing Configuration, page 37-4
- Assigning IP Addresses to Network Interfaces, page 37-5
- Configuring Address Resolution Methods, page 37-8
- Routing Assistance When IP Routing is Disabled, page 37-10
- Configuring Broadcast Packet Handling, page 37-13
- Monitoring and Maintaining IP Addressing, page 37-17

### Default Addressing Configuration

Table 37-1 shows the default addressing configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>None defined.</td>
</tr>
<tr>
<td>IP broadcast address</td>
<td>255.255.255.255 (all ones).</td>
</tr>
<tr>
<td>IP classless routing</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>
Configuring IP Addressing

Assigning IP Addresses to Network Interfaces

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.

Beginning in privileged EXEC mode, follow these steps to assign an IP address and a network mask to a Layer 3 interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>
Chapter 37 Configuring IP Unicast Routing

### Configuring IP Addressing

#### Use of Subnet Zero

Subnetting with a subnet address of zero is strongly discouraged because of the problems that can arise if a network and a subnet have the same addresses. For example, if network 131.108.0.0 is subnetted as 255.255.255.0, subnet zero would be written as 131.108.0.0, which is the same as the network address.

You can use the all ones subnet (131.108.255.0) and even though it is discouraged, you can enable the use of subnet zero if you need the entire subnet space for your IP address.

Beginning in privileged EXEC mode, follow these steps to enable subnet zero:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>no switchport</td>
<td>Remove the interface from Layer 2 configuration mode (if it is a physical interface).</td>
</tr>
<tr>
<td>4</td>
<td>ip address ip-address subnet-mask</td>
<td>Configure the IP address and IP subnet mask.</td>
</tr>
<tr>
<td>5</td>
<td>no shutdown</td>
<td>Enable the interface.</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

#### Classless Routing

By default, classless routing behavior is enabled on the switch when it is configured to route. With classless routing, if a router receives packets for a subnet of a network with no default route, the router forwards the packet to the best supernet route. A supernet consists of contiguous blocks of Class C address spaces used to simulate a single, larger address space and is designed to relieve the pressure on the rapidly depleting Class B address space.

In Figure 37-2, classless routing is enabled. When the host sends a packet to 128.20.4.1, instead of discarding the packet, the router forwards it to the best supernet route. If you disable classless routing and a router receives packets destined for a subnet of a network with no network default route, the router discards the packet.
In Figure 37-3, the router in network 128.20.0.0 is connected to subnets 128.20.1.0, 128.20.2.0, and 128.20.3.0. If the host sends a packet to 128.20.4.1, because there is no network default route, the router discards the packet.

To prevent the switch from forwarding packets destined for unrecognized subnets to the best supernet route possible, you can disable classless routing behavior.

Beginning in privileged EXEC mode, follow these steps to disable classless routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 no ip classless</td>
<td>Disable classless routing behavior.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring IP Unicast Routing

Configuring IP Addressing

To restore the default and have the switch forward packets destined for a subnet of a network with no network default route to the best supernet route possible, use the `ip classless` global configuration command.

Configuring Address Resolution Methods

You can control interface-specific handling of IP by using address resolution. A device using IP can have both a local address or MAC address, which uniquely defines the device on its local segment or LAN, and a network address, which identifies the network to which the device belongs.

The local address or MAC address is known as a data link address because it is contained in the data link layer (Layer 2) section of the packet header and is read by data link (Layer 2) devices. To communicate with a device on Ethernet, the software must learn the MAC address of the device. The process of learning the MAC address from an IP address is called *address resolution*. The process of learning the IP address from the MAC address is called *reverse address resolution*.

The switch can use these forms of address resolution:

1. **Address Resolution Protocol (ARP)** is used to associate IP address with MAC addresses. Taking an IP address as input, ARP learns the associated MAC address and then stores the IP address/MAC address association 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 or replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP).

2. **Proxy ARP** helps hosts with no routing tables learn the MAC addresses of hosts on other networks or subnets. If the switch (router) receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to the host through other interfaces, it generates a proxy ARP packet giving its own local data link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host.

The switch also uses the Reverse Address Resolution Protocol (RARP), which functions the same as ARP does, except that the RARP packets request an IP address instead of a local MAC address. Using RARP requires a RARP server on the same network segment as the router interface. Use the `ip rarp-server address` interface configuration command to identify the server.

For more information on RARP, see the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* under *Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides* from the Cisco.com page.

You can perform these tasks to configure address resolution:

- Define a Static ARP Cache, page 37-9
- Set ARP Encapsulation, page 37-9
- Enable Proxy ARP, page 37-10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entry.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To restore the default and have the switch forward packets destined for a subnet of a network with no network default route to the best supernet route possible, use the `ip classless` global configuration command.

### Configuring Address Resolution Methods

You can control interface-specific handling of IP by using address resolution. A device using IP can have both a local address or MAC address, which uniquely defines the device on its local segment or LAN, and a network address, which identifies the network to which the device belongs.

The local address or MAC address is known as a data link address because it is contained in the data link layer (Layer 2) section of the packet header and is read by data link (Layer 2) devices. To communicate with a device on Ethernet, the software must learn the MAC address of the device. The process of learning the MAC address from an IP address is called *address resolution*. The process of learning the IP address from the MAC address is called *reverse address resolution*.

The switch can use these forms of address resolution:

- **Address Resolution Protocol (ARP)** is used to associate IP address with MAC addresses. Taking an IP address as input, ARP learns the associated MAC address and then stores the IP address/MAC address association 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 or replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP).

- **Proxy ARP** helps hosts with no routing tables learn the MAC addresses of hosts on other networks or subnets. If the switch (router) receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to the host through other interfaces, it generates a proxy ARP packet giving its own local data link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host.

The switch also uses the Reverse Address Resolution Protocol (RARP), which functions the same as ARP does, except that the RARP packets request an IP address instead of a local MAC address. Using RARP requires a RARP server on the same network segment as the router interface. Use the `ip rarp-server address` interface configuration command to identify the server.

For more information on RARP, see the *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* under *Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides* from the Cisco.com page.

You can perform these tasks to configure address resolution:

- Define a Static ARP Cache, page 37-9
- Set ARP Encapsulation, page 37-9
- Enable Proxy ARP, page 37-10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entry.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To restore the default and have the switch forward packets destined for a subnet of a network with no network default route to the best supernet route possible, use the `ip classless` global configuration command.
Define a Static ARP Cache

ARP and other address resolution protocols provide dynamic mapping between IP addresses and MAC addresses. Because most hosts support dynamic address resolution, you usually do not need to specify static ARP cache entries. If you must define a static ARP cache entry, you can do so globally, which installs a permanent entry in the ARP cache that the switch uses to translate IP addresses into MAC addresses. Optionally, you can also specify that the switch respond to ARP requests as if it were the owner of the specified IP address. If you do not want the ARP entry to be permanent, you can specify a timeout period for the ARP entry.

Beginning in privileged EXEC mode, follow these steps to provide static mapping between IP addresses and MAC addresses:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>arp ip-address hardware-address type</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>arp ip-address hardware-address type [alias]</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>arp timeout seconds</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show interfaces [interface-id]</td>
</tr>
<tr>
<td>Step 8</td>
<td>show arp</td>
</tr>
<tr>
<td></td>
<td>or show ip arp</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove an entry from the ARP cache, use the **no arp ip-address hardware-address type** global configuration command. To remove all nonstatic entries from the ARP cache, use the **clear arp-cache** privileged EXEC command.

Set ARP Encapsulation

By default, Ethernet ARP encapsulation (represented by the **arpa** keyword) is enabled on an IP interface. You can change the encapsulation methods to SNAP if required by your network.
Beginning in privileged EXEC mode, follow these steps to specify the ARP encapsulation type:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
</tbody>
</table>
| Step 3 arp {arpa | snap} | Specify the ARP encapsulation method:  
  • arpa—Address Resolution Protocol  
  • snap—Subnetwork Address Protocol |
| Step 4 end                 | Return to privileged EXEC mode.                   |
| Step 5 show interfaces [interface-id] | Verify ARP encapsulation configuration on all interfaces or the specified interface. |
| Step 6 copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable an encapsulation type, use the no arp arpa or no arp snap interface configuration command.

**Enable Proxy ARP**

By default, the switch uses proxy ARP to help hosts learn MAC addresses of hosts on other networks or subnets.

Beginning in privileged EXEC mode, follow these steps to enable proxy ARP if it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 3 ip proxy-arp</td>
<td>Enable proxy ARP on the interface.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show ip interface [interface-id]</td>
<td>Verify the configuration on the interface or all interfaces.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable proxy ARP on the interface, use the no ip proxy-arp interface configuration command.

**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:

- Proxy ARP, page 37-11  
- Default Gateway, page 37-11  
- ICMP Router Discovery Protocol (IRDP), page 37-11
Proxy ARP

Proxy ARP, the most common method for learning about other routes, enables an Ethernet host with no routing information to communicate with hosts on other networks or subnets. The host assumes that all hosts are on the same local Ethernet and that they can use ARP to learn their MAC addresses. If a switch receives an ARP request for a host that is not on the same network as the sender, the switch evaluates whether it has the best route to that host. If it does, it sends an ARP reply packet with its own Ethernet MAC address, and the host that sent the request sends the packet to the switch, which forwards it to the intended host. Proxy ARP treats all networks as if they are local and performs ARP requests for every IP address.

Proxy ARP is enabled by default. To enable it after it has been disabled, see the “Enable Proxy ARP” section on page 37-10. Proxy ARP works as long as other routers support it.

Default Gateway

Another method for locating routes is to define a default router or default gateway. All nonlocal 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.

Beginning in privileged EXEC mode, follow these steps to define a default gateway (router) when IP routing is disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip default-gateway ip-address</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip redirects</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no ip default-gateway global configuration command to disable this function.

ICMP Router Discovery Protocol (IRDP)

Router discovery allows the switch to dynamically learn about routes to other networks using IRDP. IRDP allows hosts to locate routers. When operating as a host, the switch generates router discovery packets. When operating as a host, the switch receives router discovery packets. The switch can also listen to Routing Information Protocol (RIP) routing updates and use this information to infer locations of routers. The switch does not actually store the routing tables sent by routing devices; it merely keeps track of which systems are sending the data. The advantage of using IRDP is that it allows each router to specify both a priority and the time after which a device is assumed to be down if no further packets are received.

Each device discovered becomes a candidate for the default router, and a new highest-priority router is selected when a higher priority router is discovered, when the current default router is declared down, or when a TCP connection is about to time out because of excessive retransmissions.
The only required task for IRDP routing on an interface is to enable IRDP processing on that interface. When enabled, the default parameters apply. You can optionally change any of these parameters.

Beginning in privileged EXEC mode, follow these steps to enable and configure IRDP on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>interface interface-id</strong></td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configure.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ip irdp</strong></td>
<td>Enable IRDP processing on the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>ip irdp multicast</strong></td>
<td>(Optional) Send IRDP advertisements to the multicast address (224.0.0.1) instead of IP broadcasts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end-host ability before using this command.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>ip irdp holdtime seconds</strong></td>
<td>(Optional) Set the IRDP period for which advertisements are valid. The default is three times the maxadvertinterval value. It must be greater than maxadvertinterval and cannot be greater than 9000 seconds. If you change the maxadvertinterval value, this value also changes.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>ip irdp maxadvertinterval seconds</strong></td>
<td>(Optional) Set the IRDP maximum interval between advertisements. The default is 600 seconds.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>ip irdp minadvertinterval seconds</strong></td>
<td>(Optional) Set the IRDP minimum interval between advertisements. The default is 0.75 times the maxadvertinterval. If you change the maxadvertinterval, this value changes to the new default (0.75 of maxadvertinterval).</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>ip irdp preference number</strong></td>
<td>(Optional) Set a device IRDP preference level. The allowed range is $-2^{31}$ to $2^{31}$. The default is 0. A higher value increases the router preference level.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>ip irdp address address [number]</strong></td>
<td>(Optional) Specify an IRDP address and preference to proxy-advertise.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>end</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>show ip irdp</strong></td>
<td>Verify settings by displaying IRDP values.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>copy running-config startup-config</strong></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

If you change the maxadvertinterval value, the holdtime and minadvertinterval values also change, so it is important to first change the maxadvertinterval value, before manually changing either the holdtime or minadvertinterval values.

Use the no ip irdp interface configuration command to disable IRDP routing.
Configuring Broadcast Packet Handling

After configuring an IP interface address, you can enable routing and configure one or more routing protocols, or you can configure the way the switch responds to network broadcasts. A broadcast is a data packet destined for all hosts on a physical network. The switch supports two kinds of broadcasting:

- A directed broadcast packet is sent to a specific network or series of networks. A directed broadcast address includes the network or subnet fields.
- A flooded broadcast packet is sent to every network.

**Note**

You can also limit broadcast, unicast, and multicast traffic on Layer 2 interfaces by using the `storm-control` interface configuration command to set traffic suppression levels. For more information, see Chapter 23, “Configuring Port-Based Traffic Control.”

Routers provide some protection from broadcast storms by limiting their extent to the local cable. Bridges (including intelligent bridges), because they are Layer 2 devices, forward broadcasts to all network segments, thus propagating broadcast storms. The best solution to the broadcast storm problem is to use a single broadcast address scheme on a network. In most modern IP implementations, you can set the address to be used as the broadcast address. Many implementations, including the one in the switch, support several addressing schemes for forwarding broadcast messages.

Perform the tasks in these sections to enable these schemes:

- Enabling Directed Broadcast-to-Physical Broadcast Translation, page 37-13
- Forwarding UDP Broadcast Packets and Protocols, page 37-14
- Establishing an IP Broadcast Address, page 37-15
- Flooding IP Broadcasts, page 37-16

### Enabling Directed Broadcast-to-Physical Broadcast Translation

By default, IP directed broadcasts are dropped; they are not forwarded. Dropping IP-directed broadcasts makes routers less susceptible to denial-of-service attacks.

You can enable forwarding of IP-directed broadcasts on an interface where the broadcast becomes a physical (MAC-layer) broadcast. Only those protocols configured by using the `ip forward-protocol` global configuration command are forwarded.

You can specify an access list to control which broadcasts are forwarded. When an access list is specified, only those IP packets permitted by the access list are eligible to be translated from directed broadcasts to physical broadcasts. For more information on access lists, see Chapter 33, “Configuring Network Security with ACLs.”

Beginning in privileged EXEC mode, follow these steps to enable forwarding of IP-directed broadcasts on an interface:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><code>interface interface-id</code></td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
</tbody>
</table>
Configuring IP Addressing

Chapter 37 Configuring IP Unicast Routing

Configuring IP Addressing

Use the `no ip directed-broadcast` interface configuration command to disable translation of directed broadcast to physical broadcasts. Use the `no ip forward-protocol` global configuration command to remove a protocol or port.

Forwarding UDP Broadcast Packets and Protocols

User Datagram Protocol (UDP) is an IP host-to-host layer protocol, as is TCP. UDP provides a low-overhead, connectionless session between two end systems and does not provide for acknowledgment of received datagrams. Network hosts occasionally use UDP broadcasts to find address, configuration, and name information. If such a host is on a network segment that does not include a server, UDP broadcasts are normally not forwarded. You can remedy this situation by configuring an interface on a router to forward certain classes of broadcasts to a helper address. You can use more than one helper address per interface.

You can specify a UDP destination port to control which UDP services are forwarded. You can specify multiple UDP protocols. You can also specify the Network Disk (ND) protocol, which is used by older diskless Sun workstations and the network security protocol SDNS.

By default, both UDP and ND forwarding are enabled if a helper address has been defined for an interface. The description for the `ip forward-protocol` interface configuration command in the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2 lists the ports that are forwarded by default if you do not specify any UDP ports.

If you do not specify any UDP ports when you configure the forwarding of UDP broadcasts, you are configuring the router to act as a BOOTP forwarding agent. BOOTP packets carry DHCP information.

### Command Table

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip directed-broadcast [access-list-number]</td>
<td>Enable directed broadcast-to-physical broadcast translation on the interface. You can include an access list to control which broadcasts are forwarded. When an access list, only IP packets permitted by the access list can be translated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The <code>ip directed-broadcast</code> interface configuration command can be configured on a VPN routing/forwarding (VRF) interface and is VRF-aware. Directed broadcast traffic is routed only within the VRF.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip forward-protocol {udp [port]</td>
<td>nd</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>Forward UDP datagrams.</td>
</tr>
<tr>
<td></td>
<td>port: (Optional)</td>
<td>Destination port that controls which UDP services are forwarded.</td>
</tr>
<tr>
<td></td>
<td>nd</td>
<td>Forward ND datagrams.</td>
</tr>
<tr>
<td></td>
<td>ndns</td>
<td>Forward SDNS datagrams.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show ip interface [interface-id]</td>
<td>Verify the configuration on the interface or all interfaces.</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>show running-config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to enable forwarding UDP broadcast packets on an interface and specify the destination address:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip helper-address address</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip forward-protocol {udp [port]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show ip interface [interface-id]</td>
</tr>
<tr>
<td>or</td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the `no ip helper-address` interface configuration command to disable the forwarding of broadcast packets to specific addresses. Use the `no ip forward-protocol` global configuration command to remove a protocol or port.

**Establishing an IP Broadcast Address**

The most popular IP broadcast address (and the default) is an address consisting of all ones (255.255.255.255). However, the switch can be configured to generate any form of IP broadcast address.

Beginning in privileged EXEC mode, follow these steps to set the IP broadcast address on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip broadcast-address ip-address</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ip interface [interface-id]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To restore the default IP broadcast address, use the `no ip broadcast-address` interface configuration command.
Flooding IP Broadcasts

You can allow IP broadcasts to be flooded throughout your internetwork in a controlled fashion by using
the database created by the bridging STP. Using this feature also prevents loops. To support this
capability, bridging must be configured on each interface that is to participate in the flooding. If bridging
is not configured on an interface, it still can receive broadcasts. However, the interface never forwards
broadcasts it receives, and the router never uses that interface to send broadcasts received on a
different interface.

Packets that are forwarded to a single network address using the IP helper-address mechanism can be
flooded. Only one copy of the packet is sent on each network segment.

To be considered for flooding, packets must meet these criteria. (Note that these are the same conditions
used to consider packet forwarding using IP helper addresses.)

- The packet must be a MAC-level broadcast.
- The packet must be an IP-level broadcast.
- The packet must be a TFTP, DNS, Time, NetBIOS, ND, or BOOTP packet, or a UDP specified by
  the `ip forward-protocol udp` global configuration command.
- The time-to-live (TTL) value of the packet must be at least two.

A flooded UDP datagram is given the destination address specified with the `ip broadcast-address`
interface configuration command on the output interface. The destination address can be set to any
address. Thus, the destination address might change as the datagram propagates through the network.
The source address is never changed. The TTL value is decremented.

When a flooded UDP datagram is sent out an interface (and the destination address possibly changed),
the datagram is handed to the normal IP output routines and is, therefore, subject to access lists, if they
are present on the output interface.

Beginning in privileged EXEC mode, follow these steps to use the bridging spanning-tree database to
flood UDP datagrams:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip forward-protocol spanning-tree</td>
<td>Use the bridging spanning-tree database to flood UDP datagrams.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no ip forward-protocol spanning-tree` global configuration command to disable the flooding
of IP broadcasts.

In the switch, the majority of packets are forwarded in hardware; most packets do not go through the
switch CPU. For those packets that do go to the CPU, you can speed up spanning tree-based UDP
flooding by a factor of about four to five times by using turbo-flooding. This feature is supported over
Ethernet interfaces configured for ARP encapsulation.
Beginning in privileged EXEC mode, follow these steps to increase spanning-tree-based flooding:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td>2</td>
<td>ip forward-protocol turbo-flood</td>
<td>Use the spanning-tree database to speed up flooding of UDP datagrams.</td>
</tr>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>4</td>
<td>show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To disable this feature, use the `no ip forward-protocol turbo-flood` global configuration command.

### Monitoring and Maintaining IP Addressing

When the contents of a particular cache, table, or database have become or are suspected to be invalid, you can remove all its contents by using the `clear` privileged EXEC commands. Table 37-2 lists the commands for clearing contents.

**Table 37-2 Commands to Clear Caches, Tables, and Databases**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear arp-cache</td>
<td>Clear the IP ARP cache and the fast-switching cache.</td>
</tr>
<tr>
<td>clear host [name</td>
<td>Remove one or all entries from the hostname and the address cache.</td>
</tr>
<tr>
<td>clear ip route [network [mask]</td>
<td>Remove one or more routes from the IP routing table.</td>
</tr>
</tbody>
</table>

You can display specific statistics, such as the contents of IP routing tables, caches, and databases; the reachability of nodes; and the routing path that packets are taking through the network. Table 37-3 lists the privileged EXEC commands for displaying IP statistics.

**Table 37-3 Commands to Display Caches, Tables, and Databases**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show arp</td>
<td>Display the entries in the ARP table.</td>
</tr>
<tr>
<td>show hosts</td>
<td>Display the default domain name, style of lookup service, name server hosts, and the cached list of hostnames and addresses.</td>
</tr>
<tr>
<td>show ip aliases</td>
<td>Display IP addresses mapped to TCP ports (aliases).</td>
</tr>
<tr>
<td>show ip arp</td>
<td>Display the IP ARP cache.</td>
</tr>
<tr>
<td>show ip interface [interface-id]</td>
<td>Display the IP status of interfaces.</td>
</tr>
<tr>
<td>show ip rdp</td>
<td>Display IRDP values.</td>
</tr>
<tr>
<td>show ip masks [address]</td>
<td>Display the masks used for network addresses and the number of subnets using each mask.</td>
</tr>
<tr>
<td>show ip redirects</td>
<td>Display the address of a default gateway.</td>
</tr>
<tr>
<td>show ip route [address [mask]] [protocol]</td>
<td>Display the current state of the routing table.</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Display the current state of the routing table in summary form.</td>
</tr>
</tbody>
</table>
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.

Beginning in privileged EXEC mode, follow these steps to enable IP routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip routing</td>
<td>Enable IP routing.</td>
</tr>
<tr>
<td>router ip_routing_protocol</td>
<td>Specify an IP routing protocol. This step might include other commands, such as specifying the networks to route with the network (RIP) router configuration command. For information on specific protocols, see sections later in this chapter and the Cisco IOS IP Configuration Guide, Release 12.2.</td>
</tr>
</tbody>
</table>

**Note** The IP base image supports only RIP as a routing protocol

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
<th>Return to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no ip routing global configuration command to disable routing.

This example shows how to enable IP routing using RIP as the routing protocol:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# end
```

You can now set up parameters for the selected routing protocols as described in these sections:

- Configuring RIP, page 37-18
- Configuring OSPF, page 37-24
- Configuring EIGRP, page 37-33
- Configuring BGP, page 37-41
- Configuring Protocol-Independent Features, page 37-87 (optional)

Configuring RIP

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.
RIP is the only routing protocol supported by the IP base image; other routing protocols require the IP services image.

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.

These sections contain this configuration information:
- Default RIP Configuration, page 37-19
- Configuring Basic RIP Parameters, page 37-20
- Configuring RIP Authentication, page 37-21
- Configuring Summary Addresses and Split Horizon, page 37-22

### Default RIP Configuration

Table 37-4 shows the 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.</td>
</tr>
<tr>
<td></td>
<td>Authentication mode: clear text.</td>
</tr>
<tr>
<td>IP RIP receive version</td>
<td>According to the <strong>version</strong> router configuration command.</td>
</tr>
<tr>
<td>IP RIP send version</td>
<td>According to the <strong>version</strong> router configuration command.</td>
</tr>
<tr>
<td>IP RIP triggered</td>
<td>According to the <strong>version</strong> router configuration command.</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>
</tbody>
</table>
Chapter 37      Configuring IP Unicast Routing

Table 37-4   Default RIP Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<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 Catalyst 3560 switch, RIP configuration commands are ignored until you configure the network number.

Beginning in privileged EXEC mode, follow these steps to enable and configure RIP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>ip routing</td>
<td>Enable IP routing. (Required only if IP routing is disabled.)</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>router rip</td>
<td>Enable a RIP routing process, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>network network number</td>
<td>Associate 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 RIP commands to take effect.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>neighbor ip-address</td>
<td>(Optional) Define a neighboring router with which to exchange routing information. This step allows routing updates from RIP (normally a broadcast protocol) to reach nonbroadcast networks.</td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
</tr>
<tr>
<td>offset list [access-list number</td>
<td>name] [in</td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
</tr>
<tr>
<td>timers basic update invalid holddown flush</td>
<td>(Optional) Adjust routing protocol timers. Valid ranges for all timers are 0 to 4294967295 seconds. update—The time between sending routing updates. The default is 30 seconds. invalid—The timer after which a route is declared invalid. The default is 180 seconds. holddown—The time before a route is removed from the routing table. The default is 180 seconds. flush—The amount of time for which routing updates are postponed. The default is 240 seconds.</td>
</tr>
</tbody>
</table>
Configuring RIP

To turn off the RIP routing process, use the `no router rip` global configuration command.

To display the parameters and current state of the active routing protocol process, use the `show ip protocols` privileged EXEC command. Use the `show ip rip database` privileged EXEC command to display summary address entries in the RIP database.

### 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. Therefore, you must also perform the tasks in the “Managing Authentication Keys” section on page 37-101.

The switch supports two modes of authentication on interfaces for which RIP authentication is enabled: plain text and MD5. The default is plain text.

Beginning in privileged EXEC mode, follow these steps to configure RIP authentication on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
</tbody>
</table>
Configuring RIP

To restore clear text authentication, use the `no ip rip authentication mode` interface configuration command. To prevent authentication, use the `no ip rip authentication key-chain` interface configuration command.

Configuring 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.

**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.

Beginning in privileged EXEC mode, follow these steps to set an interface to advertise a summarized local IP address and to disable split horizon on the interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip address ip-address subnet-mask</code> Configure the IP address and IP subnet.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ip summary-address rip ip address ip-network mask</code> Configure the IP address to be summarized and the IP network mask.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>no ip split horizon</code> Disable split horizon on the interface.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show ip interface interface-id</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To disable IP summarization, use the `no ip summary-address rip` router configuration command.

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)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

### 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.

Beginning in privileged EXEC mode, follow these steps to disable split horizon on the interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip address ip-address subnet-mask</code> Configure the IP address and IP subnet.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>no ip split-horizon</code> Disable split horizon on the interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>show ip interface interface-id</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To enable the split horizon mechanism, use the `ip split-horizon` interface configuration command.
Configuring OSPF

This section briefly describes how to configure Open Shortest Path First (OSPF). For a complete description of the OSPF commands, see the “OSPF Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2* from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

**Note**

OSPF classifies different media into broadcast, nonbroadcast, and point-to-point networks. The switch supports broadcast (Ethernet, Token Ring, and FDDI) and point-to-point networks (Ethernet interfaces configured as point-to-point links).

OSPF is an Interior Gateway Protocol (IGP) designed expressly for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. The Cisco implementation supports RFC 1253, OSPF management information base (MIB).

The Cisco implementation conforms to the OSPF Version 2 specifications with these key features:

- Definition of stub areas is supported.
- Routes learned through any IP routing protocol can be redistributed into another IP routing protocol. At the intradomain level, this means that OSPF can import routes learned through EIGRP and RIP. OSPF routes can also be exported into RIP.
- Plain text and MD5 authentication among neighboring routers within an area is supported.
- Configurable routing interface parameters include interface output cost, retransmission interval, interface transmit delay, router priority, router dead and hello intervals, and authentication key.
- Virtual links are supported.
- Not-so-stubby-areas (NSSAs) per RFC 1587 are supported.

OSPF typically requires coordination among many internal routers, area border routers (ABRs) connected to multiple areas, and autonomous system boundary routers (ASBRs). The minimum configuration would use all default parameter values, no authentication, and interfaces assigned to areas. If you customize your environment, you must ensure coordinated configuration of all routers.

These sections contain this configuration information:

- Default OSPF Configuration, page 37-25
- Configuring Basic OSPF Parameters, page 37-27
- Configuring OSPF Interfaces, page 37-27
- Configuring OSPF Area Parameters, page 37-29
- Configuring Other OSPF Parameters, page 37-30
- Changing LSA Group Pacing, page 37-32
- Configuring a Loopback Interface, page 37-32
- Monitoring OSPF, page 37-33

**Note**

To enable OSPF, the switch must be running the IP services image.
## Default OSPF Configuration

Table 37-5 shows the default OSPF configuration.

### Table 37-5 Default OSPF Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface parameters</td>
<td>Cost: No default cost predefined.</td>
</tr>
<tr>
<td></td>
<td>Retransmit interval: 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>Transmit delay: 1 second.</td>
</tr>
<tr>
<td></td>
<td>Priority: 1.</td>
</tr>
<tr>
<td></td>
<td>Hello interval: 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Dead interval: 4 times the hello interval.</td>
</tr>
<tr>
<td></td>
<td>No authentication.</td>
</tr>
<tr>
<td></td>
<td>No password specified.</td>
</tr>
<tr>
<td></td>
<td>MD5 authentication disabled.</td>
</tr>
<tr>
<td></td>
<td>Area Authentication type: 0 (no authentication).</td>
</tr>
<tr>
<td></td>
<td>Default cost: 1.</td>
</tr>
<tr>
<td></td>
<td>Range: Disabled.</td>
</tr>
<tr>
<td></td>
<td>Stub: No stub area defined.</td>
</tr>
<tr>
<td></td>
<td>NSSA: No NSSA area defined.</td>
</tr>
<tr>
<td></td>
<td>Auto cost: 100 Mbs/s.</td>
</tr>
<tr>
<td>Default-information originate</td>
<td>Disabled. When enabled, the default metric setting is 10, and the external route type default is Type 2.</td>
</tr>
<tr>
<td>Default metric</td>
<td>Built-in, automatic metric translation, as appropriate for each routing protocol.</td>
</tr>
<tr>
<td>Distance OSPF</td>
<td>dist1 (all routes within an area): 110.</td>
</tr>
<tr>
<td></td>
<td>dist2 (all routes from one area to another): 110.</td>
</tr>
<tr>
<td></td>
<td>and dist3 (routes from other routing domains): 110.</td>
</tr>
<tr>
<td>OSPF database filter</td>
<td>Disabled. All outgoing link-state advertisements (LSAs) are flooded to the interface.</td>
</tr>
<tr>
<td>IP OSPF name lookup</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Log adjacency changes</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>None specified.</td>
</tr>
<tr>
<td>Neighbor database filter</td>
<td>Disabled. All outgoing LSAs are flooded to the neighbor.</td>
</tr>
<tr>
<td>Network area</td>
<td>Disabled.</td>
</tr>
<tr>
<td>NSF1 awareness</td>
<td>Enabled for switches running the IP services image.</td>
</tr>
<tr>
<td></td>
<td>Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes.</td>
</tr>
<tr>
<td>Router ID</td>
<td>No OSPF routing process defined.</td>
</tr>
</tbody>
</table>
Chapter 37 Configuring IP Unicast Routing

### Configuring OSPF

**OSPF for Routed Access**

With Cisco IOS Release 12.2(55)SE, the IP Base image supports OSPF for routed access. The IP services image is required if you need multiple OSPFv2 and OSPFv3 instances without route restrictions. Additionally, the IP services image is required to enable the multi-VRF-CE feature.

OSPF for Routed Access is specifically designed so that you can extend Layer 3 routing capabilities to the wiring closet.

**Note**

OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a combined total of 200 dynamically learned routes. The IP Base image provides OSPF for routed access. However, these restrictions are not enforced in this release.

With the typical topology (hub and spoke) in a campus environment, where the wiring closets (spokes) are connected to the distribution switch (hub) that forwards all nonlocal traffic to the distribution layer, the wiring closet switch need not hold a complete routing table. A best practice design, where the distribution switch sends a default route to the wiring closet switch to reach interarea and external routes (OSPF stub or totally stub area configuration) should be used when OSPF for Routed Access is used in the wiring closet.

For more details, go to:


**OSPF NSF Awareness**

The IP services image supports OSPF NSF Awareness for IPv4. When a neighboring router is NSF-capable, the Layer 3 switch continues to forward packets from the router before the backup Route Processor (RP) in a router takes over after the primary RP fails, or while the primary RP is manually reloaded for a nondisruptive software upgrade.

---

### Table 37-5 Default OSPF Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary address</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Timers LSA group pacing</td>
<td>240 seconds.</td>
</tr>
<tr>
<td>Timers shortest path first (spf)</td>
<td>spf delay: 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>spf-holdtime: 10 seconds.</td>
</tr>
<tr>
<td>Virtual link</td>
<td>No area ID or router ID defined.</td>
</tr>
<tr>
<td></td>
<td>Hello interval: 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Retransmit interval: 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>Transmit delay: 1 second.</td>
</tr>
<tr>
<td></td>
<td>Dead interval: 40 seconds.</td>
</tr>
<tr>
<td></td>
<td>Authentication key: no key predefined.</td>
</tr>
<tr>
<td></td>
<td>Message-digest key (MD5): no key predefined.</td>
</tr>
</tbody>
</table>

1. NSF = Nonstop forwarding
This feature cannot be disabled. For more information on this feature, see the OSPF Nonstop Forwarding (NSF) Awareness Feature Guide:

### Configuring Basic OSPF Parameters

Enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range.

Beginning in privileged EXEC mode, follow these steps to enable OSPF:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router ospf process-id</td>
<td>Enable OSPF routing, and enter router configuration mode. The process ID is an internally used identification parameter that is locally assigned and can be any positive integer. Each OSPF routing process has a unique value.</td>
</tr>
<tr>
<td>Step 3 network address wildcard-mask area area-id</td>
<td>Define an interface on which OSPF runs and the area ID for that interface. You can use the wildcard mask as a single command to define one or more interfaces to be associated with a specific OSPF area. The area ID can be a decimal value or an IP address.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show ip protocols</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To end an OSPF routing process, use the no router ospf process-id global configuration command.

This example shows how to configure an OSPF routing process and assign it a process number of 109:

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

### Configuring OSPF Interfaces

You can use the ip ospf interface configuration commands to modify interface-specific OSPF parameters. You are not required to modify any of these parameters, but some interface parameters (hello interval, dead interval, and authentication key) must be consistent across all routers in an attached network. If you modify these parameters, be sure all routers in the network have compatible values.

**Note** The ip ospf interface configuration commands are all optional.
Beginning in privileged EXEC mode, follow these steps to modify OSPF interface parameters:

<table>
<thead>
<tr>
<th>Command</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> interface <em>interface-id</em></td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip ospf cost</td>
<td>(Optional) Explicitly specify the cost of sending a packet on the interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip ospf retransmit-interval <em>seconds</em></td>
<td>(Optional) Specify the number of seconds between link state advertisement transmissions. The range is 1 to 65535 seconds. The default is 5 seconds.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip ospf transmit-delay <em>seconds</em></td>
<td>(Optional) Set the estimated number of seconds to wait before sending a link state update packet. The range is 1 to 65535 seconds. The default is 1 second.</td>
</tr>
<tr>
<td><strong>Step 6</strong> ip ospf priority <em>number</em></td>
<td>(Optional) Set priority to help find the OSPF designated router for a network. The range is from 0 to 255. The default is 1.</td>
</tr>
<tr>
<td><strong>Step 7</strong> ip ospf hello-interval <em>seconds</em></td>
<td>(Optional) Set the number of seconds between hello packets sent on an OSPF interface. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 10 seconds.</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip ospf dead-interval <em>seconds</em></td>
<td>(Optional) Set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 4 times the hello interval.</td>
</tr>
<tr>
<td><strong>Step 9</strong> ip ospf authentication-key <em>key</em></td>
<td>(Optional) Assign a password to be used by neighboring OSPF routers. The password can be any string of keyboard-entered characters up to 8 bytes in length. All neighboring routers on the same network must have the same password to exchange OSPF information.</td>
</tr>
</tbody>
</table>
| **Step 10** ip ospf message digest-key *keyid* md5 *key* | (Optional) Enable MDS authentication.  
  - *keyid*—An identifier from 1 to 255.  
  - *key*—An alphanumeric password of up to 16 bytes. |
| **Step 11** ip ospf database-filter all out | (Optional) Block flooding of OSPF LSA packets to the interface. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. |
| **Step 12** end | Return to privileged EXEC mode.                                      |
| **Step 13** show ip ospf interface [*interface-name*] | Display OSPF-related interface information. |
Chapter 37 Configuring IP Unicast Routing

Configuring OSPF

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area, but can import AS external routes within the area by redistribution.

Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the area range router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.

Note

The OSPF area router configuration commands are all optional.

Beginning in privileged EXEC mode, follow these steps to configure area parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>router ospf process-id</td>
<td>Enable OSPF routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>area area-id authentication</td>
<td>(Optional) Allow password-based protection against unauthorized access to the identified area. The identifier can be either a decimal value or an IP address.</td>
</tr>
<tr>
<td>area area-id authentication message-digest</td>
<td>(Optional) Enable MD5 authentication on the area.</td>
</tr>
<tr>
<td>area area-id stub [no-summary]</td>
<td>(Optional) Define an area as a stub area. The no-summary keyword prevents an ABR from sending summary link advertisements into the stub area.</td>
</tr>
</tbody>
</table>
### Configuring Other OSPF Parameters

You can optionally configure other OSPF parameters in router configuration mode.

- **Route summarization:** When redistributing routes from other protocols as described in the “Using Route Maps to Redistribute Routing Information” section on page 37-91, each route is advertised individually in an external LSA. To help decrease the size of the OSPF link state database, you can use the `summary-address` router configuration command to advertise a single router for all the redistributed routes included in a specified network address and mask.

- **Virtual links:** In OSPF, all areas must be connected to a backbone area. You can establish a virtual link in case of a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and the nonbackbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.

- **Default route:** When you specifically configure redistribution of routes into an OSPF routing domain, the route automatically becomes an autonomous system boundary router (ASBR). You can force the ASBR to generate a default route into the OSPF routing domain.

- **Default Name Server (DNS) names for use in all OSPF show privileged EXEC command displays makes it easier to identify a router than displaying it by router ID or neighbor ID.

- **Default Metrics:** OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface. The metric is calculated as `ref-bw` divided by bandwidth, where `ref` is 10 by default, and bandwidth (`bw`) is specified by the `bandwidth` interface configuration command. For multiple links with high bandwidth, you can specify a larger number to differentiate the cost on those links.

---

### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 6    | `area area-id nssa [no-redistribution] [default-information-originate] [no-summary]` | (Optional) Defines an area as a not-so-stubby-area. Every router within the same area must agree that the area is NSSA. Select one of these keywords:  
  - `no-redistribution`—Select when the router is an NSSA ABR and you want the `redistribute` command to import routes into normal areas, but not into the NSSA.  
  - `default-information-originate`—Select on an ABR to allow importing type 7 LSAs into the NSSA.  
  - `no-redistribution`—Select to not send summary LSAs into the NSSA. |
| 7    | `area area-id range address mask` | (Optional) Specify an address range for which a single route is advertised. Use this command only with area border routers. |
| 8    | `end` | Return to privileged EXEC mode. |
| 9    | `show ip ospf [process-id]` | Display information about the OSPF routing process in general or for a specific process ID to verify configuration. |
|      | `show ip ospf [process-id [area-id]] database` | Display lists of information related to the OSPF database for a specific router. |
| 10   | `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

Use the `no` form of these commands to remove the configured parameter value or to return to the default value.
Administrative distance is a rating of the trustworthiness of a routing information source, an integer between 0 and 255, with a higher value meaning a lower trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. OSPF uses three different administrative distances: routes within an area (interarea), routes to another area (interarea), and routes from another routing domain learned through redistribution (external). You can change any of the distance values.

Passive interfaces: Because interfaces between two devices on an Ethernet represent only one network segment, to prevent OSPF from sending hello packets for the sending interface, you must configure the sending device to be a passive interface. Both devices can identify each other through the hello packet for the receiving interface.

Route calculation timers: You can configure the delay time between when OSPF receives a topology change and when it starts the shortest path first (SPF) calculation and the hold time between two SPF calculations.

Log neighbor changes: You can configure the router to send a syslog message when an OSPF neighbor state changes, providing a high-level view of changes in the router.

Beginning in privileged EXEC mode, follow these steps to configure these OSPF parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router ospf process-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>summary-address address mask</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>area area-id virtual-link router-id [hello-interval seconds] [retransmit-interval seconds] [trans] [[authentication-key key]</td>
</tr>
<tr>
<td></td>
<td>[message-digest-key keyid md5 key]]</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ip ospf name-lookup</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>ip auto-cost reference-bandwidth ref-bw</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>distance ospf [[inter-area dist1] [inter-area dist2] [external dist3]]</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>passive-interface type number</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>timers throttle spf spf-delay spf-holdtime spf-wait</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>ospf log-adj-changes</td>
</tr>
</tbody>
</table>
Configuring OSPF

Changing LSA Group Pacing

The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, check-summing, and aging functions for more efficient router use. This feature is enabled by default with a 4-minute default pacing interval, and you will not usually need to modify this parameter. The optimum group pacing interval is inversely proportional to the number of LSAs the router is refreshing, check-summing, and aging. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Beginning in privileged EXEC mode, follow these steps to configure OSPF LSA pacing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip ospf [process-id [area-id]] database</td>
<td>Display lists of information related to the OSPF database for a specific router. For some of the keyword options, see the “Monitoring OSPF” section on page 37-33.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default value, use the no timers lsa-group-pacing router configuration command.

Configuring a Loopback Interface

OSPF uses the highest IP address configured on the interfaces as its router ID. If this interface is down or removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces. If a loopback interface is configured with an IP address, OSPF uses this IP address as its router ID, even if other interfaces have higher IP addresses. Because loopback interfaces never fail, this provides greater stability. OSPF automatically prefers a loopback interface over other interfaces, and it chooses the highest IP address among all loopback interfaces.

Beginning in privileged EXEC mode, follow these steps to configure a loopback interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>router ospf process-id</td>
<td>Enable OSPF routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>timers lsa-group-pacing seconds</td>
<td>Change the group pacing of LSAs.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Step

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface loopback 0</td>
<td>Create a loopback interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>ip address address mask</td>
<td>Assign an IP address to this interface.</td>
</tr>
</tbody>
</table>
Use the `no interface loopback 0` global configuration command to disable the loopback interface.

**Monitoring OSPF**

You can display specific statistics such as the contents of IP routing tables, caches, and databases.

Table 37-6 lists some of the privileged EXEC commands for displaying statistics. For more `show ip ospf database` privileged EXEC command options and for explanations of fields in the resulting display, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ospf [process-id] database [router] [link-state-id]</code></td>
<td>Display lists of information related to the OSPF database.</td>
</tr>
<tr>
<td><code>show ip ospf [process-id] database [router] [self-originate]</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf [process-id] database [router] [adv-router [ip-address]]</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf [process-id] database [network] [link-state-id]</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf [process-id] database [summary] [link-state-id]</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf [process-id] database [asbr-summary] [link-state-id]</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf [process-id] database [external] [link-state-id]</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf [process-id area-id] database [database-summary]</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf border-routes</code></td>
<td>Display the internal OSPF routing ABR and ASBR table entries.</td>
</tr>
<tr>
<td><code>show ip ospf interface [interface-name]</code></td>
<td>Display OSPF-related interface information.</td>
</tr>
<tr>
<td><code>show ip ospf neighbor [interface-name] [neighbor-id] detail</code></td>
<td>Display OSPF interface neighbor information.</td>
</tr>
<tr>
<td><code>show ip ospf virtual-links</code></td>
<td>Display OSPF-related virtual links information.</td>
</tr>
</tbody>
</table>

**Configuring EIGRP**

Enhanced IGRP (EIGRP) is a Cisco proprietary enhanced version of the IGRP. EIGRP uses the same distance vector algorithm and distance information as IGRP; however, the convergence properties and the operating efficiency of EIGRP are significantly improved.

The convergence technology employs an algorithm referred to as the Diffusing Update Algorithm (DUAL), which guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations.
IP EIGRP provides increased network width. With RIP, the largest possible width of your network is 15 hops. Because the EIGRP metric is large enough to support thousands of hops, the only barrier to expanding the network is the transport-layer hop counter. EIGRP increments the transport control field only when an IP packet has traversed 15 routers and the next hop to the destination was learned through EIGRP. When a RIP route is used as the next hop to the destination, the transport control field is incremented as usual.

EIGRP offers these features:

- Fast convergence.
- Incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table, minimizing the bandwidth required for EIGRP packets.
- Less CPU usage because full update packets need not be processed each time they are received.
- Protocol-independent neighbor discovery mechanism to learn about neighboring routers.
- Variable-length subnet masks (VLSMs).
- Arbitrary route summarization.
- EIGRP scales to large networks.

EIGRP has these four basic components:

- Neighbor discovery and recovery is the process that routers use to dynamically learn of other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. Neighbor discovery and recovery is achieved with low overhead by periodically sending small hello packets. As long as hello packets are received, the Cisco IOS software can learn that a neighbor is alive and functioning. When this status is determined, the neighboring routers can exchange routing information.

- The reliable transport protocol is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. It supports intermixed transmission of multicast and unicast packets. Some EIGRP packets must be sent reliably, and others need not be. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities (such as Ethernet), it is not necessary to send hellos reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello with an indication in the packet informing the receivers that the packet need not be acknowledged. Other types of packets (such as updates) require acknowledgment, which is shown in the packet. The reliable transport has a provision to send multicast packets quickly when there are unacknowledged packets pending. Doing so helps ensure that convergence time remains low in the presence of varying speed links.

- The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses the distance information (known as a metric) to select efficient, loop-free paths. DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors, but there are neighbors advertising the destination, a recomputation must occur. This is the process whereby a new successor is determined. The amount of time it takes to recompute the route affects the convergence time. Recomputation is processor-intensive; it is advantageous to avoid recomputation if it is not necessary. When a topology change occurs, DUAL tests for feasible successors. If there are feasible successors, it uses any it finds to avoid unnecessary recomputation.

- The protocol-dependent modules are responsible for network layer protocol-specific tasks. An example is the IP EIGRP module, which is responsible for sending and receiving EIGRP packets that are encapsulated in IP. It is also responsible for parsing EIGRP packets and informing DUAL of the new information received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IP routing table. EIGRP is also responsible for redistributing routes learned by other IP routing protocols.
These sections contain this configuration information:

- Default EIGRP Configuration, page 37-35
- Configuring Basic EIGRP Parameters, page 37-37
- Configuring EIGRP Interfaces, page 37-38
- Configuring EIGRP Route Authentication, page 37-38
- Configuring EIGRP Stub Routing, page 37-39
- Monitoring and Maintaining EIGRP, page 37-41

**Note**

To enable EIGRP, the switch must be running the IP services image.

### Default EIGRP Configuration

Table 37-7 shows the default EIGRP configuration.

**Table 37-7  Default EIGRP Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto summary</td>
<td>Enabled. Subprefixes are summarized to the classful network boundary when crossing classful network boundaries.</td>
</tr>
<tr>
<td>Default-information</td>
<td>Exterior routes are accepted and default information is passed between EIGRP processes when doing redistribution.</td>
</tr>
<tr>
<td>Default metric</td>
<td>Only connected routes and interface static routes can be redistributed without a default metric. The metric includes:</td>
</tr>
<tr>
<td></td>
<td>• Bandwidth: 0 or greater kb/s.</td>
</tr>
<tr>
<td></td>
<td>• Delay (tens of microseconds): 0 or any positive number that is a multiple of 39.1 nanoseconds.</td>
</tr>
<tr>
<td></td>
<td>• Reliability: any number between 0 and 255 (255 means 100 percent reliability).</td>
</tr>
<tr>
<td></td>
<td>• Loading: effective bandwidth as a number between 0 and 255 (255 is 100 percent loading).</td>
</tr>
<tr>
<td></td>
<td>• MTU: maximum transmission unit size of the route in bytes. 0 or any positive integer.</td>
</tr>
<tr>
<td>Distance</td>
<td>Internal distance: 90.</td>
</tr>
<tr>
<td></td>
<td>External distance: 170.</td>
</tr>
<tr>
<td>EIGRP log-neighbor changes</td>
<td>Disabled. No adjacency changes logged.</td>
</tr>
<tr>
<td>IP authentication key-chain</td>
<td>No authentication provided.</td>
</tr>
<tr>
<td>IP authentication mode</td>
<td>No authentication provided.</td>
</tr>
<tr>
<td>IP bandwidth-percent</td>
<td>50 percent.</td>
</tr>
<tr>
<td>IP hello interval</td>
<td>For low-speed nonbroadcast multiaccess (NBMA) networks: 60 seconds; all other networks: 5 seconds.</td>
</tr>
<tr>
<td>IP hold-time</td>
<td>For low-speed NBMA networks: 180 seconds; all other networks: 15 seconds.</td>
</tr>
</tbody>
</table>
Configuring EIGRP

To create an EIGRP routing process, you must enable EIGRP and associate networks. EIGRP sends updates to the interfaces in the specified networks. If you do not specify an interface network, it is not advertised in any EIGRP update.

### Table 37-7 Default EIGRP Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP split-horizon</td>
<td>Enabled.</td>
</tr>
<tr>
<td>IP summary address</td>
<td>No summary aggregate addresses are predefined.</td>
</tr>
<tr>
<td>Metric weights</td>
<td>tos: 0; k1 and k3: 1; k2, k4, and k5: 0</td>
</tr>
<tr>
<td>Network</td>
<td>None specified.</td>
</tr>
<tr>
<td>NSF1 Awareness</td>
<td>Enabled for switches running the IP services image.</td>
</tr>
<tr>
<td></td>
<td>Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes.</td>
</tr>
<tr>
<td>Offset-list</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Router EIGRP</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Set metric</td>
<td>No metric set in the route map.</td>
</tr>
<tr>
<td>Traffic-share</td>
<td>Distributed proportionately to the ratios of the metrics.</td>
</tr>
<tr>
<td>Variance</td>
<td>1 (equal-cost load balancing).</td>
</tr>
</tbody>
</table>

1. NSF = Nonstop Forwarding

To create an EIGRP routing process, you must enable EIGRP and associate networks. EIGRP sends updates to the interfaces in the specified networks. If you do not specify an interface network, it is not advertised in any EIGRP update.

If you have routers on your network that are configured for IGRP, and you want to change to EIGRP, you must designate transition routers that have both IGRP and EIGRP configured. In these cases, perform Steps 1 through 3 in the next section and also see the “Configuring Split Horizon” section on page 37-23. You must use the same AS number for routes to be automatically redistributed.

### EIGRP NSF Awareness

The EIGRP NSF Awareness feature is supported for IPv4 in the IP services image. When the neighboring router is NSF-capable, the Layer 3 switch continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router failing and the backup RP taking over, or while the primary RP is manually reloaded for a nondisruptive software upgrade.

This feature cannot be disabled. For more information on this feature, see the *EIGRP Nonstop Forwarding (NSF) Awareness Feature Guide*:

## Configuring Basic EIGRP Parameters

Beginning in privileged EXEC mode, follow these steps to configure EIGRP. Configuring the routing process is required; other steps are optional:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>router eigrp autonomous-system number</td>
<td>Enable an EIGRP routing process, and enter router configuration mode. The AS number identifies the routes to other EIGRP routers and tags routing information.</td>
</tr>
<tr>
<td>3</td>
<td>network network-number</td>
<td>Associate networks with an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks.</td>
</tr>
<tr>
<td>4</td>
<td>eigrp log-neighbor-changes</td>
<td>(Optional) Enable logging of EIGRP neighbor changes to monitor routing system stability.</td>
</tr>
</tbody>
</table>
| 5    | metric weights tos k1 k2 k3 k4 k5 | (Optional) Adjust the EIGRP metric. Although the defaults have been carefully set to provide excellent operation in most networks, you can adjust them.  

**Caution** Setting metrics is complex and is not recommended without guidance from an experienced network designer. |
| 6    | offset list [access-list number | (Optional) Apply an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through EIGRP. You can limit the offset list with an access list or an interface. |
|      | name] {in | out} |   |
|      | offset [type number] |   |
| 7    | no auto-summary | (Optional) Disable automatic summarization of subnet routes into network-level routes. |
| 8    | ip summary-address eigrp autonomous-system-number address mask | (Optional) Configure a summary aggregate. |
| 9    | end | Return to privileged EXEC mode. |
| 10   | show ip protocols | Verify your entries. |
| 11   | show ip protocols | Verify your entries.  
For NSF awareness, the output shows:  
*** IP Routing is NSF aware ***  
EIGRP NSF enabled |
| 12   | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the `no` forms of these commands to disable the feature or return the setting to the default value.
Configuring EIGRP Interfaces

Other optional EIGRP parameters can be configured on an interface basis.

Beginning in privileged EXEC mode, follow these steps to configure EIGRP interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip bandwidth-percent eigrp percent</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip summary-address eigrp autonomous-system-number address mask</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>ip hello-interval eigrp autonomous-system-number seconds</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ip hold-time eigrp autonomous-system-number seconds</td>
</tr>
</tbody>
</table>

⚠️ **Caution** Do not adjust the hold time without consulting Cisco technical support. |

| **Step 7** | no ip split-horizon eigrp autonomous-system-number | (Optional) Disable split horizon to allow route information to be advertised by a router out any interface from which that information originated. |
| **Step 8** | end | Return to privileged EXEC mode. |
| **Step 9** | show ip eigrp interface | Display which interfaces EIGRP is active on and information about EIGRP relating to those interfaces. |
| **Step 10** | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the **no** forms of these commands to disable the feature or return the setting to the default value.

Configuring EIGRP Route Authentication

EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol to prevent the introduction of unauthorized or false routing messages from unapproved sources.
Beginning in privileged EXEC mode, follow these steps to enable authentication:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1  | configure terminal
         | Enter global configuration mode. |
| Step 2  | interface interface-id
         | Enter interface configuration mode, and specify the Layer 3 interface to configure. |
| Step 3  | ip authentication mode eigrp autonomous-system md5
         | Enable MD5 authentication in IP EIGRP packets. |
| Step 4  | ip authentication key-chain eigrp autonomous-system key-chain
         | Enable authentication of IP EIGRP packets. |
| Step 5  | exit
         | Return to global configuration mode. |
| Step 6  | key chain name-of-chain
         | Identify a key chain and enter key-chain configuration mode. Match the name configured in Step 4. |
| Step 7  | key number
         | In key-chain configuration mode, identify the key number. |
| Step 8  | key-string text
         | In key-chain key configuration mode, identify the key string. |
| Step 9  | accept-lifetime start-time {infinite | end-time | duration seconds}
         | (Optional) Specify the time period during which the key can be received. |
         | The start-time and end-time syntax can be either hh:mm:ss Month date year or hh:mm:ss date Month year. The default is forever with the default start-time and the earliest acceptable date as January 1, 1993. The default end-time and duration is infinite. |
| Step 10 | send-lifetime start-time {infinite | end-time | duration seconds}
         | (Optional) Specify the time period during which the key can be sent. |
         | The start-time and end-time syntax can be either hh:mm:ss Month date year or hh:mm:ss date Month year. The default is forever with the default start-time and the earliest acceptable date as January 1, 1993. The default end-time and duration is infinite. |
| Step 11 | end
         | Return to privileged EXEC mode. |
| Step 12 | show key chain
         | Display authentication key information. |
| Step 13 | copy running-config startup-config
         | (Optional) Save your entries in the configuration file. |

Use the no forms of these commands to disable the feature or to return the setting to the default value.

**Configuring EIGRP Stub Routing**

The EIGRP stub routing feature, available in all images, reduces resource utilization by moving routed traffic closer to the end user.

**Note** The IP base image contains only EIGRP stub routing capability, which only advertises connected or summary routes from the routing tables to other switches in the network. The switch uses EIGRP stub routing at the access layer to eliminate the need for other types of routing advertisements. For enhanced...
capability and complete EIGRP routing, the switch must be running the IP services image. On a switch running the IP base image, if you try to configure multi-VRF-CE and EIGRP stub routing at the same time, the configuration is not allowed.

In a network using EIGRP stub routing, the only allowable route for IP traffic to the user is through a switch that is configured with EIGRP stub routing. The switch sends the routed traffic to interfaces that are configured as user interfaces or are connected to other devices.

When using EIGRP stub routing, you need to configure the distribution and remote routers to use EIGRP and to configure only the switch as a stub. Only specified routes are propagated from the switch. The switch responds to all queries for summaries, connected routes, and routing updates.

Any neighbor that receives a packet informing it of the stub status does not query the stub router for any routes, and a router that has a stub peer does not query that peer. The stub router depends on the distribution router to send the proper updates to all peers.

In Figure 37-4, switch B is configured as an EIGRP stub router. Switches A and C are connected to the rest of the WAN. Switch B advertises connected, static, redistribution, and summary routes to switch A and C. Switch B does not advertise any routes learned from switch A (and the reverse).

**Figure 37-4  EIGRP Stub Router Configuration**

![EIGRP Stub Router Configuration Diagram]

Note After you have entered the `eigrp stub` router configuration command, only the `eigrp stub connected summary` command takes effect. Although the CLI help might show the `receive-only` and `static` keywords and the you can enter these keywords, the switch running the IP base image always behaves as if the `connected` and `summary` keywords were configured.

Monitoring and Maintaining EIGRP

You can delete neighbors from the neighbor table. You can also display various EIGRP routing statistics. Table 37-8 lists the privileged EXEC commands for deleting neighbors and displaying statistics. For explanations of fields in the resulting display, see the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

Table 37-8  IP EIGRP Clear and Show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip eigrp neighbors [if-address</td>
<td>interface]</td>
</tr>
<tr>
<td>show ip eigrp interface [interface] [as number]</td>
<td>Display information about interfaces configured for EIGRP.</td>
</tr>
<tr>
<td>show ip eigrp neighbors [type-number]</td>
<td>Display EIGRP discovered neighbors.</td>
</tr>
<tr>
<td>show ip eigrp topology [autonomous-system-number]</td>
<td>Display the EIGRP topology table for a given process.</td>
</tr>
<tr>
<td>show ip eigrp traffic [autonomous-system-number]</td>
<td>Display the number of packets sent and received for all or a specified EIGRP process.</td>
</tr>
</tbody>
</table>

Configuring BGP

The Border Gateway Protocol (BGP) is an exterior gateway protocol used to set up an interdomain routing system that guarantees the loop-free exchange of routing information between autonomous systems. Autonomous systems are made up of routers that operate under the same administration and that run Interior Gateway Protocols (IGPs), such as RIP or OSPF, within their boundaries and that interconnect by using an Exterior Gateway Protocol (EGP). BGP Version 4 is the standard EGP for interdomain routing in the Internet. The protocol is defined in RFCs 1163, 1267, and 1771. You can find detailed information about BGP in Internet Routing Architectures, published by Cisco Press, and in the “Configuring BGP” chapter in the Cisco IP and IP Routing Configuration Guide from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Configuration Guides.

For details about BGP commands and keywords, see the “IP Routing Protocols” part of the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2 under Documentation > Cisco IOS Software > 12.2 Mainline > Command References. For a list of BGP commands that are visible but not supported by the switch, see Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”

Routers that belong to the same autonomous system (AS) and that exchange BGP updates run internal BGP (IBGP), and routers that belong to different autonomous systems and that exchange BGP updates run external BGP (EBGP). Most configuration commands are the same for configuring EBGP and IBGP. The difference is that the routing updates are exchanged either between autonomous systems (EBGP) or within an AS (IBGP). Figure 37-5 shows a network that is running both EBGP and IBGP.
Before exchanging information with an external AS, BGP ensures that networks within the AS can be reached by defining internal BGP peering among routers within the AS and by redistributing BGP routing information to IGPs that run within the AS, such as IGRP and OSPF.

Routers that run a BGP routing process are often referred to as BGP speakers. BGP uses the Transmission Control Protocol (TCP) as its transport protocol (specifically port 179). Two BGP speakers that have a TCP connection to each other for exchanging routing information are known as peers or neighbors. In Figure 37-5, Routers A and B are BGP peers, as are Routers B and C and Routers C and D. The routing information is a series of AS numbers that describe the full path to the destination network. BGP uses this information to construct a loop-free map of autonomous systems.

The network has these characteristics:

- Routers A and B are running EBGP, and Routers B and C are running IBGP. Note that the EBGP peers are directly connected and that the IBGP peers are not. As long as there is an IGP running that allows the two neighbors to reach one another, IBGP peers do not have to be directly connected.
- All BGP speakers within an AS must establish a peer relationship with each other. That is, the BGP speakers within an AS must be fully meshed logically. BGP4 provides two techniques that reduce the requirement for a logical full mesh: confederations and route reflectors.
- AS 200 is a transit AS for AS 100 and AS 300—that is, AS 200 is used to transfer packets between AS 100 and AS 300.

BGP peers initially exchange their full BGP routing tables and then send only incremental updates. BGP peers also exchange keepalive messages (to ensure that the connection is up) and notification messages (in response to errors or special conditions).

In BGP, each route consists of a network number, a list of autonomous systems that information has passed through (the autonomous system path), and a list of other path attributes. The primary function of a BGP system is to exchange network reachability information, including information about the list of AS paths, with other BGP systems. This information can be used to determine AS connectivity, to prune routing loops, and to enforce AS-level policy decisions.

A router or switch running Cisco IOS does not select or use an IBGP route unless it has a route available to the next-hop router and it has received synchronization from an IGP (unless IGP synchronization is disabled). When multiple routes are available, BGP bases its path selection on attribute values. See the “Configuring BGP Decision Attributes” section on page 37-50 for information about BGP attributes.
BGP Version 4 supports classless interdomain routing (CIDR) so you can reduce the size of your routing tables by creating aggregate routes, resulting in supernets. CIDR eliminates the concept of network classes within BGP and supports the advertising of IP prefixes.

These sections contain this configuration information:

- Default BGP Configuration, page 37-43
- Enabling BGP Routing, page 37-46
- Managing Routing Policy Changes, page 37-48
- Configuring BGP Decision Attributes, page 37-50
- Configuring BGP Filtering with Route Maps, page 37-52
- Configuring BGP Filtering by Neighbor, page 37-52
- Configuring Prefix Lists for BGP Filtering, page 37-54
- Configuring BGP Community Filtering, page 37-55
- Configuring BGP Neighbors and Peer Groups, page 37-56
- Configuring Aggregate Addresses, page 37-58
- Configuring Routing Domain Confederations, page 37-59
- Configuring BGP Route Reflectors, page 37-59
- Configuring Route Dampening, page 37-60
- Monitoring and Maintaining BGP, page 37-61


For a list of BGP commands that are visible but not supported by the switch, see Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”

### Default BGP Configuration

Table 37-9 shows the basic default BGP configuration. For the defaults for all characteristics, see the specific commands in the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate address</td>
<td>Disabled: None defined.</td>
</tr>
<tr>
<td>AS path access list</td>
<td>None defined.</td>
</tr>
<tr>
<td>Auto summary</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Best path</td>
<td>• The router considers as-path in choosing a route and does not compare similar routes from external BGP peers.</td>
</tr>
<tr>
<td></td>
<td>• Compare router ID: Disabled.</td>
</tr>
</tbody>
</table>
### Table 37-9  Default BGP Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP community list</td>
<td>• Number: None defined. When you permit a value for the community number, the</td>
</tr>
<tr>
<td></td>
<td>list defaults to an implicit deny for everything else that has not been permitted.</td>
</tr>
<tr>
<td></td>
<td>• Format: Cisco default format (32-bit number).</td>
</tr>
<tr>
<td>BGP confederation identifier/peers</td>
<td>• Identifier: None configured.</td>
</tr>
<tr>
<td></td>
<td>• Peers: None identified.</td>
</tr>
<tr>
<td>BGP Fast external fallover</td>
<td>Enabled.</td>
</tr>
<tr>
<td>BGP local preference</td>
<td>100. The range is 0 to 4294967295 with the higher value preferred.</td>
</tr>
<tr>
<td>BGP network</td>
<td>None specified; no backdoor route advertised.</td>
</tr>
<tr>
<td>BGP route dampening</td>
<td>Disabled by default. When enabled:</td>
</tr>
<tr>
<td></td>
<td>• Half-life is 15 minutes.</td>
</tr>
<tr>
<td></td>
<td>• Re-use is 750 (10-second increments).</td>
</tr>
<tr>
<td></td>
<td>• Suppress is 2000 (10-second increments).</td>
</tr>
<tr>
<td></td>
<td>• Max-suppress-time is 4 times half-life; 60 minutes.</td>
</tr>
<tr>
<td>BGP router ID</td>
<td>The IP address of a loopback interface if one is configured or the highest IP</td>
</tr>
<tr>
<td></td>
<td>address configured for a physical interface on the router.</td>
</tr>
<tr>
<td>Default information originate</td>
<td>Disabled.</td>
</tr>
<tr>
<td>(protocol or network redistribution)</td>
<td></td>
</tr>
<tr>
<td>Default metric</td>
<td>Built-in, automatic metric translations.</td>
</tr>
<tr>
<td>Distance</td>
<td>• External route administrative distance: 20 (acceptable values are from 1 to 255).</td>
</tr>
<tr>
<td></td>
<td>• Internal route administrative distance: 200 (acceptable values are from 1 to 255).</td>
</tr>
<tr>
<td></td>
<td>• Local route administrative distance: 200 (acceptable values are from 1 to 255).</td>
</tr>
<tr>
<td>Distribute list</td>
<td>• In (filter networks received in updates): Disabled.</td>
</tr>
<tr>
<td></td>
<td>• Out (suppress networks from being advertised in updates): Disabled.</td>
</tr>
<tr>
<td>Internal route redistribution</td>
<td>Disabled.</td>
</tr>
<tr>
<td>IP prefix list</td>
<td>None defined.</td>
</tr>
<tr>
<td>Multi exit discriminator (MED)</td>
<td>• Always compare: Disabled. Does not compare MEDs for paths from neighbors in</td>
</tr>
<tr>
<td></td>
<td>different autonomous systems.</td>
</tr>
<tr>
<td></td>
<td>• Best path compare: Disabled.</td>
</tr>
<tr>
<td></td>
<td>• MED missing as worst path: Disabled.</td>
</tr>
<tr>
<td></td>
<td>• Deterministic MED comparison is disabled.</td>
</tr>
</tbody>
</table>
## Configuring BGP

### Table 37-9  Default BGP Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>- Advertisement interval: 30 seconds for external peers; 5 seconds for internal peers.</td>
</tr>
<tr>
<td></td>
<td>- Change logging: Enabled.</td>
</tr>
<tr>
<td></td>
<td>- Conditional advertisement: Disabled.</td>
</tr>
<tr>
<td></td>
<td>- Default originate: No default route is sent to the neighbor.</td>
</tr>
<tr>
<td></td>
<td>- Description: None.</td>
</tr>
<tr>
<td></td>
<td>- Distribute list: None defined.</td>
</tr>
<tr>
<td></td>
<td>- External BGP multihop: Only directly connected neighbors are allowed.</td>
</tr>
<tr>
<td></td>
<td>- Filter list: None used.</td>
</tr>
<tr>
<td></td>
<td>- Maximum number of prefixes received: No limit.</td>
</tr>
<tr>
<td></td>
<td>- Next hop (router as next hop for BGP neighbor): Disabled.</td>
</tr>
<tr>
<td></td>
<td>- Password: Disabled.</td>
</tr>
<tr>
<td></td>
<td>- Peer group: None defined; no members assigned.</td>
</tr>
<tr>
<td></td>
<td>- Prefix list: None specified.</td>
</tr>
<tr>
<td></td>
<td>- Remote AS (add entry to neighbor BGP table): No peers defined.</td>
</tr>
<tr>
<td></td>
<td>- Private AS number removal: Disabled.</td>
</tr>
<tr>
<td></td>
<td>- Route maps: None applied to a peer.</td>
</tr>
<tr>
<td></td>
<td>- Send community attributes: None sent to neighbors.</td>
</tr>
<tr>
<td></td>
<td>- Shutdown or soft reconfiguration: Not enabled.</td>
</tr>
<tr>
<td></td>
<td>- Timers: keepalive: 60 seconds; holdtime: 180 seconds.</td>
</tr>
<tr>
<td></td>
<td>- Update source: Best local address.</td>
</tr>
<tr>
<td></td>
<td>- Weight: Routes learned through BGP peer: 0; routes sourced by the local router: 32768.</td>
</tr>
<tr>
<td><strong>NSF(^1)</strong> Awareness</td>
<td>Disable. Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> NSF Awareness can be enabled for IPv4 on switches with the IP services image by enabling Graceful Restart.</td>
</tr>
<tr>
<td>Route reflector</td>
<td>None configured.</td>
</tr>
<tr>
<td>Synchronization (BGP and IGP)</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Table map update</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Timers</td>
<td>Keepalive: 60 seconds; holdtime: 180 seconds.</td>
</tr>
</tbody>
</table>

1. NSF = Nonstop Forwarding
Nonstop Forwarding Awareness

The BGP NSF Awareness feature is supported for IPv4 in the IP services image. To enable this feature with BGP routing, you need to enable Graceful Restart. When the neighboring router is NSF-capable, and this feature is enabled, the Layer 3 switch continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router failing and the backup RP taking over, or while the primary RP is manually reloaded for a nondisruptive software upgrade.

For more information, see the BGP Nonstop Forwarding (NSF) Awareness Feature Guide: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftbgpnsf.html

Enabling BGP Routing

To enable BGP routing, you establish a BGP routing process and define the local network. Because BGP must completely recognize the relationships with its neighbors, you must also specify a BGP neighbor.

BGP supports two kinds of neighbors: internal and external. Internal neighbors are in the same AS; external neighbors are in different autonomous systems. External neighbors are usually adjacent to each other and share a subnet, but internal neighbors can be anywhere in the same AS.

The switch supports the use of private AS numbers, usually assigned by service providers and given to systems whose routes are not advertised to external neighbors. The private AS numbers are from 64512 to 65535. You can configure external neighbors to remove private AS numbers from the AS path by using the neighbor remove-private-as router configuration command. Then when an update is passed to an external neighbor, if the AS path includes private AS numbers, these numbers are dropped.

If your AS will be passing traffic through it from another AS to a third AS, it is important to be consistent about the routes it advertises. If BGP advertised a route before all routers in the network had learned about the route through the IGP, the AS might receive traffic that some routers could not yet route. To prevent this from happening, BGP must wait until the IGP has propagated information across the AS so that BGP is synchronized with the IGP. Synchronization is enabled by default. If your AS does not pass traffic from one AS to another AS, or if all routers in your autonomous systems are running BGP, you can disable synchronization, which allows your network to carry fewer routes in the IGP and allows BGP to converge more quickly.

Note

To enable BGP, the switch must be running the IP services image.

Beginning in privileged EXEC mode, follow these steps to enable BGP routing, establish a BGP routing process, and specify a neighbor:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip routing Enable IP routing (required only if IP routing is disabled).</td>
</tr>
<tr>
<td>Step 3</td>
<td>router bgp autonomous-system Enable a BGP routing process, assign it an AS number, and enter router configuration mode. The AS number can be from 1 to 65535, with 64512 to 65535 designated as private autonomous numbers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>network network-number [mask network-mask] [route-map route-map-name] Configure a network as local to this AS, and enter it in the BGP table.</td>
</tr>
</tbody>
</table>
### Command Purpose

| Step 5 | `neighbor {ip-address | peer-group-name} remote-as number` | Add an entry to the BGP neighbor table specifying that the neighbor identified by the IP address belongs to the specified AS.  
For EBGP, neighbors are usually directly connected, and the IP address is the address of the interface at the other end of the connection.  
For IBGP, the IP address can be the address of any of the router interfaces. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>`neighbor {ip-address</td>
<td>peer-group-name} remove-private-as`</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>no synchronization</code></td>
<td>(Optional) Disable synchronization between BGP and an IGP.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>no auto-summary</code></td>
<td>(Optional) Disable automatic network summarization. By default, when a subnet is redistributed from an IGP into BGP, only the network route is inserted into the BGP table.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>bgp fast-external-fallover</code></td>
<td>(Optional) Automatically reset a BGP session when a link between external neighbors goes down. By default, the session is not immediately reset.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>bgp graceful-restart</code></td>
<td>(Optional) Enable NSF awareness on switch. By default, NSF awareness is disabled.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| Step 12 | `show ip bgp network network-number` or `show ip bgp neighbor` | Verify the configuration.  
Verify that NSF awareness (Graceful Restart) is enabled on the neighbor.  
If NSF awareness is enabled on the switch and the neighbor, this message appears:  

Graceful Restart Capability: advertised and received  
If NSF awareness is enabled on the switch, but not on the neighbor, this message appears:  

Graceful Restart Capability: advertised |
| Step 13 | `copy running-config startup-config` | (Optional) Save your entries in the configuration file. |

Use the `no router bgp autonomous-system` global configuration command to remove a BGP AS. Use the `no network network-number` router configuration command to remove the network from the BGP table. Use the `no neighbor {ip-address | peer-group-name} remote-as number` router configuration command to remove a neighbor. Use the `no neighbor {ip-address | peer-group-name} remove-private-as` router configuration command to include private AS numbers in updates to a neighbor. Use the `synchronization` router configuration command to re-enable synchronization.
These examples show how to configure BGP on the routers in Figure 37-5.

Router A:
```
Switch(config)# router bgp 100
Switch(config-router)# neighbor 129.213.1.1 remote-as 200
```

Router B:
```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 129.213.1.2 remote-as 100
Switch(config-router)# neighbor 175.220.1.2 remote-as 200
```

Router C:
```
Switch(config)# router bgp 200
Switch(config-router)# neighbor 175.220.212.1 remote-as 200
Switch(config-router)# neighbor 192.208.10.1 remote-as 300
```

Router D:
```
Switch(config)# router bgp 300
Switch(config-router)# neighbor 192.208.10.2 remote-as 200
```

To verify that BGP peers are running, use the `show ip bgp neighbors` privileged EXEC command. This is the output of this command on Router A:
```
Switch# show ip bgp neighbors
BGP neighbor is 129.213.1.1, remote AS 200, external link
BGP version 4, remote router ID 175.220.212.1
BGP state = established, table version = 3, up for 0:10:59
Last read 0:00:29, hold time is 180, keepalive interval is 60 seconds
Minimum time between advertisement runs is 30 seconds
Received 2828 messages, 0 notifications, 0 in queue
Sent 2826 messages, 0 notifications, 0 in queue
Connections established 11; dropped 10
```

Anything other than `state = established` means that the peers are not running. The remote router ID is the highest IP address on that router (or the highest loopback interface). Each time the table is updated with new information, the table version number increments. A table version number that continually increments means that a route is flapping, causing continual routing updates.

For exterior protocols, a reference to an IP network from the `network` router configuration command controls only which networks are advertised. This is in contrast to Interior Gateway Protocols (IGPs), such as EIGRP, which also use the `network` command to specify where to send updates.

For detailed descriptions of BGP configuration, see the “IP Routing Protocols” part of the *Cisco IOS IP Configuration Guide, Release 12.2*. For details about specific commands, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2*. See Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE,” for a list of BGP commands that are visible but not supported by the switch.

### Managing Routing Policy Changes

Routing policies for a peer include all the configurations that might affect inbound or outbound routing table updates. When you have defined two routers as BGP neighbors, they form a BGP connection and exchange routing information. If you later change a BGP filter, weight, distance, version, or timer, or make a similar configuration change, you must reset the BGP sessions so that the configuration changes take effect.
There are two types of reset, hard reset and soft reset. The switch supports a soft reset without any prior configuration. To use a soft reset without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the OPEN message sent when the peers establish a TCP session. A soft reset allows the dynamic exchange of route refresh requests and routing information between BGP routers and the subsequent re-advertisement of the respective outbound routing table.

- When soft reset generates inbound updates from a neighbor, it is called *dynamic inbound soft reset*.
- When soft reset sends a set of updates to a neighbor, it is called *outbound soft reset*.

A soft inbound reset causes the new inbound policy to take effect. A soft outbound reset causes the new local outbound policy to take effect without resetting the BGP session. As a new set of updates is sent during outbound policy reset, a new inbound policy can also take effect.

Table 37-10 lists the advantages and disadvantages of hard and soft resets.

<table>
<thead>
<tr>
<th>Type of Reset</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard reset</td>
<td>No memory overhead</td>
<td>The prefixes in the BGP, IP, and FIB tables provided by the neighbor are lost. Not recommended.</td>
</tr>
<tr>
<td>Outbound soft reset</td>
<td>No configuration, no storing of routing table updates</td>
<td>Does not reset inbound routing table updates.</td>
</tr>
<tr>
<td>Dynamic inbound soft reset</td>
<td>Does not clear the BGP session and cache</td>
<td>Both BGP routers must support the route refresh capability.</td>
</tr>
<tr>
<td></td>
<td>Does not require storing of routing table updates and has no memory overhead</td>
<td></td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to learn if a BGP peer supports the route refresh capability and to reset the BGP session:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | show ip bgp neighbors          | Display whether a neighbor supports the route refresh capability. When supported, this message appears for the router:  
Received route refresh capability from peer. |
| Step 2 | clear ip bgp [{* | address | peer-group-name}] | Reset the routing table on the specified connection.  
• Enter an asterisk (*) to specify that all connections be reset.  
• Enter an IP address to specify the connection to be reset.  
• Enter a peer group name to reset the peer group. |
| Step 3 | clear ip bgp [{* | address | peer-group-name}] soft out | (Optional) Perform an outbound soft reset to reset the inbound routing table on the specified connection. Use this command if route refresh is supported.  
• Enter an asterisk (*) to specify that all connections be reset.  
• Enter an IP address to specify the connection to be reset.  
• Enter a peer group name to reset the peer group. |
| Step 4 | show ip bgp  
show ip bgp neighbors | Verify the reset by checking information about the routing table and about BGP neighbors. |
Chapter 37      Configuring IP Unicast Routing

Configuring BGP Decision Attributes

When a BGP speaker receives updates from multiple autonomous systems that describe different paths to the same destination, it must choose the single best path for reaching that destination. When chosen, the selected path is entered into the BGP routing table and propagated to its neighbors. The decision is based on the value of attributes that the update contains and other BGP-configurable factors.

When a BGP peer learns two EBGP paths for a prefix from a neighboring AS, it chooses the best path and inserts that path in the IP routing table. If BGP multipath support is enabled and the EBGP paths are learned from the same neighboring autonomous systems, instead of a single best path, multiple paths are installed in the IP routing table. Then, during packet switching, per-packet or per-destination load balancing is performed among the multiple paths. The `maximum-paths` router configuration command controls the number of paths allowed.

These factors summarize the order in which BGP evaluates the attributes for choosing the best path:

1. If the path specifies a next hop that is inaccessible, drop the update. The BGP next-hop attribute, automatically determined by the software, is the IP address of the next hop that is going to be used to reach a destination. For EBGP, this is usually the IP address of the neighbor specified by the `neighbor remote-as` router configuration command. You can disable next-hop processing by using route maps or the `neighbor next-hop-self` router configuration command.
2. Prefer the path with the largest weight (a Cisco proprietary parameter). The weight attribute is local to the router and not propagated in routing updates. By default, the weight attribute is 32768 for paths that the router originates and zero for other paths. Routes with the largest weight are preferred. You can use access lists, route maps, or the `neighbor weight` router configuration command to set weights.
3. Prefer the route with the highest local preference. Local preference is part of the routing update and exchanged among routers in the same AS. The default value of the local preference attribute is 100. You can set local preference by using the `bgp default local-preference` router configuration command or by using a route map.
4. Prefer the route that was originated by BGP running on the local router.
5. Prefer the route with the shortest AS path.
6. Prefer the route with the lowest origin type. An interior route or IGP is lower than a route learned by EGP, and an EGP-learned route is lower than one of unknown origin or learned in another way.
7. Prefer the route with the lowest multi-exit discriminator (MED) metric attribute if the neighboring AS is the same for all routes considered. You can configure the MED by using route maps or by using the `default-metric` router configuration command. When an update is sent to an IBGP peer, the MED is included.
8. Prefer the external (EBGP) path over the internal (IBGP) path.
9. Prefer the route that can be reached through the closest IGP neighbor (the lowest IGP metric). This means that the router will prefer the shortest internal path within the AS to reach the destination (the shortest path to the BGP next-hop).
10. If the following conditions are all true, insert the route for this path into the IP routing table:
    - Both the best route and this route are external.
    - Both the best route and this route are from the same neighboring autonomous system.
    - `maximum-paths` is enabled.
11. If multipath is not enabled, prefer the route with the lowest IP address value for the BGP router ID. The router ID is usually the highest IP address on the router or the loopback (virtual) address, but might be implementation-specific.
Beginning in privileged EXEC mode, follow these steps to configure some decision attributes:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router bgp autonomous-system</code> Enable a BGP routing process, assign it an AS number, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>bgp best-path as-path ignore</code> (Optional) Configure the router to ignore AS path length in selecting a route.</td>
</tr>
<tr>
<td>Step 4</td>
<td>`neighbor {ip-address</td>
</tr>
<tr>
<td>Step 5</td>
<td>`neighbor {ip-address</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>default-metric number</code> (Optional) Set a MED metric to set preferred paths to external neighbors. All routes without a MED will also be set to this value. The range is 1 to 4294967295. The lowest value is the most desirable.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>bgp bestpath med missing-as-worst</code> (Optional) Configure the switch to consider a missing MED as having a value of infinity, making the path without a MED value the least desirable path.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>bgp always-compare med</code> (Optional) Configure the switch to compare MEDs for paths from neighbors in different autonomous systems. By default, MED comparison is only done among paths in the same AS.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>bgp bestpath med confed</code> (Optional) Configure the switch to consider the MED in choosing a path from among those advertised by different subautonomous systems within a confederation.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>bgp deterministic med</code> (Optional) Configure the switch to consider the MED variable when choosing among routes advertised by different peers in the same AS.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>bgp default local-preference value</code> (Optional) Change the default local preference value. The range is 0 to 4294967295; the default value is 100. The highest local preference value is preferred.</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>maximum-paths number</code> (Optional) Configure the number of paths to be added to the IP routing table. The default is to only enter the best path in the routing table. The range is from 1 to 16. Having multiple paths allows load balancing among the paths. (Although the switch software allows a maximum of 32 equal-cost routes, the switch hardware will never use more than 16 paths per route.)</td>
</tr>
<tr>
<td>Step 13</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 14</td>
<td><code>show ip bgp show ip bgp neighbors</code> Verify the reset by checking information about the routing table and about BGP neighbors.</td>
</tr>
<tr>
<td>Step 15</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Configuring BGP Filtering with Route Maps

Within BGP, route maps can be used to control and to modify routing information and to define the conditions by which routes are redistributed between routing domains. See the “Using Route Maps to Redistribute Routing Information” section on page 37-91 for more information about route maps. Each route map has a name that identifies the route map (map tag) and an optional sequence number.

Beginning in privileged EXEC mode, follow these steps to use a route map to disable next-hop processing:

1. **configure terminal**
   - Enter global configuration mode.

2. **route-map map-tag [permit | deny] [sequence-number]**
   - Create a route map, and enter route-map configuration mode.

3. **set ip next-hop ip-address […ip-address] [peer-address]**
   - (Optional) Set a route map to disable next-hop processing
     - In an inbound route map, set the next hop of matching routes to be the neighbor peering address, overriding third-party next hops.
     - In an outbound route map of a BGP peer, set the next hop to the peering address of the local router, disabling the next-hop calculation.

4. **end**
   - Return to privileged EXEC mode.

5. **show route-map [map-name]**
   - Display all route maps configured or only the one specified to verify configuration.

6. **copy running-config startup-config**
   - (Optional) Save your entries in the configuration file.

Use the **no route-map map-tag** command to delete the route map. Use the **no set ip next-hop ip-address** command to re-enable next-hop processing.

Configuring BGP Filtering by Neighbor

You can filter BGP advertisements by using AS-path filters, such as the **as-path access-list** global configuration command and the **neighbor filter-list** router configuration command. You can also use access lists with the **neighbor distribute-list** router configuration command. Distribute-list filters are applied to network numbers. See the “Controlling Advertising and Processing in Routing Updates” section on page 37-100 for information about the **distribute-list** command.

You can use route maps on a per-neighbor basis to filter updates and to modify various attributes. A route map can be applied to either inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates. On both inbound and outbound updates, matching is supported based on AS path, community, and network numbers. Autonomous system path matching requires the **match as-path access-list** route-map command, community based matching requires the **match community-list** route-map command, and network-based matching requires the **ip access-list** global configuration command.
Beginning in privileged EXEC mode, follow these steps to apply a per-neighbor route map:

<table>
<thead>
<tr>
<th>Command</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> router bgp autonomous-system</td>
<td>Enable a BGP routing process, assign it an AS number, and enter router configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 3** neighbor {ip-address \ peer-group name} distribute-list \ access-list-number \ name} {in \ out} | (Optional) Filter BGP routing updates to or from neighbors as specified in an access list.  
  **Note** You can also use the **neighbor prefix-list** router configuration command to filter updates, but you cannot use both commands to configure the same BGP peer. |
| **Step 4** neighbor {ip-address \ peer-group name} route-map map-tag \ in \ out} | (Optional) Apply a route map to filter an incoming or outgoing route. |
| **Step 5** end                  | Return to privileged EXEC mode.                                          |
| **Step 6** show ip bgp neighbors | Verify the configuration.                                               |
| **Step 7** copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the **no neighbor distribute-list** command to remove the access list from the neighbor. Use the **no neighbor route-map map-tag** router configuration command to remove the route map from the neighbor.

Another method of filtering is to specify an access list filter on both incoming and outbound updates, based on the BGP autonomous system paths. Each filter is an access list based on regular expressions. (See the “Regular Expressions” appendix in the *Cisco IOS Dial Technologies Command Reference, Release 12.2* for more information on forming regular expressions.) To use this method, define an autonomous system path access list, and apply it to updates to and from particular neighbors.

Beginning in privileged EXEC mode, follow these steps to configure BGP path filtering:

<table>
<thead>
<tr>
<th>Command</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> ip as-path access-list access-list-number {permit \ deny} as-regular-expressions</td>
<td>Define a BGP-related access list.</td>
</tr>
<tr>
<td><strong>Step 3</strong> router bgp autonomous-system</td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> neighbor {ip-address \ peer-group name} filter-list \ access-list-number \ name} {in \ out \ weight weight}</td>
<td>Establish a BGP filter based on an access list.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show ip bgp neighbors [paths regular-expression]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 7</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Configuring Prefix Lists for BGP Filtering

You can use prefix lists as an alternative to access lists in many BGP route filtering commands, including the `neighbor distribute-list` router configuration command. The advantages of using prefix lists include performance improvements in loading and lookup of large lists, incremental update support, easier CLI configuration, and greater flexibility.

Filtering by a prefix list involves matching the prefixes of routes with those listed in the prefix list, as when matching access lists. When there is a match, the route is used. Whether a prefix is permitted or denied is based upon these rules:

- An empty prefix list permits all prefixes.
- An implicit deny is assumed if a given prefix does not match any entries in a prefix list.
- When multiple entries of a prefix list match a given prefix, the sequence number of a prefix list entry identifies the entry with the lowest sequence number.

By default, sequence numbers are generated automatically and incremented in units of five. If you disable the automatic generation of sequence numbers, you must specify the sequence number for each entry. You can specify sequence values in any increment. If you specify increments of one, you cannot insert additional entries into the list; if you choose very large increments, you might run out of values.

You do not need to specify a sequence number when removing a configuration entry. Show commands include the sequence numbers in their output.

Before using a prefix list in a command, you must set up the prefix list. Beginning in privileged EXEC mode, follow these steps to create a prefix list or to add an entry to a prefix list:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Create a prefix list with an optional sequence number to deny or permit access for matching conditions. You must enter at least one permit or deny clause.</td>
</tr>
</tbody>
</table>
| `ip prefix-list list-name [seq seq-value] deny | permit network/len [ge ge-value] [le le-value]` | - `network/len` is the network number and length (in bits) of the network mask.  
- (Optional) `ge` and `le` values specify the range of the prefix length to be matched. The specified `ge-value` and `le-value` must satisfy this condition: `len < ge-value < le-value < 32` |
| **Step 3** | (Optional) Add an entry to a prefix list, and assign a sequence number to the entry. |
| `ip prefix-list list-name seq seq-value deny | permit network/len [ge ge-value] [le le-value]` | |
| **Step 4** | Return to privileged EXEC mode. |
| `end` | |
| **Step 5** | Verify the configuration by displaying information about a prefix list or prefix list entries. |
| `show ip prefix-list [detail | summary] name [network/len] [seq seq-num] [longer] [first-match]` | |
| **Step 6** | (Optional) Save your entries in the configuration file. |
| `copy running-config startup-config` | |

To delete a prefix list and all of its entries, use the `no ip prefix-list list-name` global configuration command. To delete an entry from a prefix list, use the `no ip prefix-list seq seq-value` global configuration command. To disable automatic generation of sequence numbers, use the `no ip prefix-list`
sequence number command; to reenable automatic generation, use the `ip prefix-list sequence number` command. To clear the hit-count table of prefix list entries, use the `clear ip prefix-list` privileged EXEC command.

### Configuring BGP Community Filtering

One way that BGP controls the distribution of routing information based on the value of the COMMUNITIES attribute. The attribute is a way to groups destinations into communities and to apply routing decisions based on the communities. This method simplifies configuration of a BGP speaker to control distribution of routing information.

A community is a group of destinations that share some common attribute. Each destination can belong to multiple communities. AS administrators can define to which communities a destination belongs. By default, all destinations belong to the general Internet community. The community is identified by the COMMUNITIES attribute, an optional, transitive, global attribute in the numerical range from 1 to 4294967200. These are some predefined, well-known communities:

- **internet**—Advertise this route to the Internet community. All routers belong to it.
- **no-export**—Do not advertise this route to EBGP peers.
- **no-advertise**—Do not advertise this route to any peer (internal or external).
- **local-as**—Do not advertise this route to peers outside the local autonomous system.

Based on the community, you can control which routing information to accept, prefer, or distribute to other neighbors. A BGP speaker can set, append, or modify the community of a route when learning, advertising, or redistributing routes. When routes are aggregated, the resulting aggregate has a COMMUNITIES attribute that contains all communities from all the initial routes.

You can use community lists to create groups of communities to use in a match clause of a route map. As with an access list, a series of community lists can be created. Statements are checked until a match is found. As soon as one statement is satisfied, the test is concluded.

To set the COMMUNITIES attribute and match clauses based on communities, see the **match community-list** and **set community** route-map configuration commands in the “Using Route Maps to Redistribute Routing Information” section on page 37-91.

By default, no COMMUNITIES attribute is sent to a neighbor. You can specify that the COMMUNITIES attribute be sent to the neighbor at an IP address by using the **neighbor send-community** router configuration command.

Beginning in privileged EXEC mode, follow these steps to create and to apply a community list:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`ip community-list community-list-number {permit</td>
<td>deny} community-number`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>community-list-number</code> is an integer from 1 to 99 that identifies one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <code>community-number</code> is the number configured by a <code>set community</code> route-map configuration command.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>router bgp autonomous-system</code></td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`neighbor {ip-address</td>
<td>peer-group name} send-community`</td>
</tr>
</tbody>
</table>
## Configuring BGP Neighbors and Peer Groups

Often many BGP neighbors are configured with the same update policies (that is, the same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and to make updating more efficient. When you have configured many peers, we recommend this approach.

To configure a BGP peer group, you create the peer group, assign options to the peer group, and add neighbors as peer group members. You configure the peer group by using the `neighbor` router configuration commands. By default, peer group members inherit all the configuration options of the peer group, including the remote-as (if configured), version, update-source, out-route-map, out-filter-list, out-dist-list, minimum-advertisement-interval, and next-hop-self. All peer group members also inherit changes made to the peer group. Members can also be configured to override the options that do not affect outbound updates.

To assign configuration options to an individual neighbor, specify any of these router configuration commands by using the neighbor IP address. To assign the options to a peer group, specify any of the commands by using the peer group name. You can disable a BGP peer or peer group without removing all the configuration information by using the `neighbor shutdown` router configuration command.

Beginning in privileged EXEC mode, use these commands to configure BGP peers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>router bgp autonomous-system</td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>neighbor peer-group-name peer-group</td>
<td>Create a BGP peer group.</td>
</tr>
<tr>
<td>4</td>
<td>neighbor ip-address peer-group peer-group-name</td>
<td>Make a BGP neighbor a member of the peer group.</td>
</tr>
<tr>
<td>5</td>
<td>neighbor {ip-address</td>
<td>peer-group-name} remote-as number</td>
</tr>
<tr>
<td>6</td>
<td>neighbor {ip-address</td>
<td>peer-group-name} description text</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>neighbor [ip-address \ peer-group-name] default-originate [route-map map-name]</code></td>
<td>(Optional) Allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.</td>
</tr>
<tr>
<td>8</td>
<td><code>neighbor [ip-address \ peer-group-name] send-community</code></td>
<td>(Optional) Specify that the COMMUNITIES attribute be sent to the neighbor at this IP address.</td>
</tr>
<tr>
<td>9</td>
<td><code>neighbor [ip-address \ peer-group-name] update-source interface</code></td>
<td>(Optional) Allow internal BGP sessions to use any operational interface for TCP connections.</td>
</tr>
<tr>
<td>10</td>
<td><code>neighbor [ip-address \ peer-group-name] ebgp-multihop</code></td>
<td>(Optional) Allow BGP sessions, even when the neighbor is not on a directly connected segment. The multihop session is not established if the only route to the multihop peer’s address is the default route (0.0.0.0).</td>
</tr>
<tr>
<td>11</td>
<td><code>neighbor [ip-address \ peer-group-name] local-as number</code></td>
<td>(Optional) Specify an AS number to use as the local AS. The range is 1 to 65535.</td>
</tr>
<tr>
<td>12</td>
<td><code>neighbor [ip-address \ peer-group-name] advertisement-interval seconds</code></td>
<td>(Optional) Set the minimum interval between sending BGP routing updates.</td>
</tr>
<tr>
<td>13</td>
<td><code>neighbor [ip-address \ peer-group-name] maximum-prefix maximum [threshold]</code></td>
<td>(Optional) Control how many prefixes can be received from a neighbor. The range is 1 to 4294967295. The <code>threshold</code> (optional) is the percentage of maximum at which a warning message is generated. The default is 75 percent.</td>
</tr>
<tr>
<td>14</td>
<td><code>neighbor [ip-address \ peer-group-name] next-hop-self</code></td>
<td>(Optional) Disable next-hop processing on the BGP updates to a neighbor.</td>
</tr>
<tr>
<td>15</td>
<td><code>neighbor [ip-address \ peer-group-name] password string</code></td>
<td>(Optional) Set MD5 authentication on a TCP connection to a BGP peer. The same password must be configured on both BGP peers, or the connection between them is not made.</td>
</tr>
<tr>
<td>16</td>
<td>`neighbor [ip-address \ peer-group-name] route-map map-name [in</td>
<td>out]`</td>
</tr>
<tr>
<td>17</td>
<td><code>neighbor [ip-address \ peer-group-name] send-community</code></td>
<td>(Optional) Specify that the COMMUNITIES attribute be sent to the neighbor at this IP address.</td>
</tr>
</tbody>
</table>
| 18   | `neighbor [ip-address \ peer-group-name] timers keepalive holdtime` | (Optional) Set timers for the neighbor or peer group.  
- The `keepalive` interval is the time within which keepalive messages are sent to peers. The range is 1 to 4294967295 seconds; the default is 60.  
- The `holdtime` is the interval after which a peer is declared inactive after not receiving a keepalive message from it. The range is 1 to 4294967295 seconds; the default is 180. |
| 19   | `neighbor [ip-address \ peer-group-name] weight weight` | (Optional) Specify a weight for all routes from a neighbor. |
| 20   | `neighbor [ip-address \ peer-group-name] distribute-list {access-list-number | name} [in | out]` | (Optional) Filter BGP routing updates to or from neighbors, as specified in an access list. |
| 21   | `neighbor [ip-address \ peer-group-name] filter-list access-list-number {in | out | weight weight}` | (Optional) Establish a BGP filter. |
| 22   | `neighbor [ip-address \ peer-group-name] version value` | (Optional) Specify the BGP version to use when communicating with a neighbor. |
To disable an existing BGP neighbor or neighbor peer group, use the `neighbor shutdown` router configuration command. To enable a previously existing neighbor or neighbor peer group that had been disabled, use the `no neighbor shutdown` router configuration command.

### Configuring Aggregate Addresses

Classless interdomain routing (CIDR) enables you to create aggregate routes (or *supernets*) to minimize the size of routing tables. You can configure aggregate routes in BGP either by redistributing an aggregate route into BGP or by creating an aggregate entry in the BGP routing table. An aggregate address is added to the BGP table when there is at least one more specific entry in the BGP table.

Beginning in privileged EXEC mode, use these commands to create an aggregate address in the routing table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router bgp autonomous-system</td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>Step 3 aggregate-address address mask</td>
<td>Create an aggregate entry in the BGP routing table. The aggregate route is advertised as coming from the AS, and the atomic aggregate attribute is set to indicate that information might be missing.</td>
</tr>
<tr>
<td>Step 4 aggregate-address address mask as-set</td>
<td>(Optional) Generate AS set path information. This command creates an aggregate entry following the same rules as the previous command, but the advertised path will be an AS_SET consisting of all elements contained in all paths. Do not use this keyword when aggregating many paths because this route must be continually withdrawn and updated.</td>
</tr>
<tr>
<td>Step 5 aggregate-address address-mask summary-only</td>
<td>(Optional) Advertise summary addresses only.</td>
</tr>
<tr>
<td>Step 6 aggregate-address address mask</td>
<td>(Optional) Suppress selected, more specific routes.</td>
</tr>
<tr>
<td>suppress-map map-name</td>
<td></td>
</tr>
<tr>
<td>Step 7 aggregate-address address mask</td>
<td>(Optional) Generate an aggregate based on conditions specified by the route map.</td>
</tr>
<tr>
<td>advertise-map map-name</td>
<td></td>
</tr>
<tr>
<td>Step 8 aggregate-address address mask</td>
<td>(Optional) Generate an aggregate with attributes specified in the route map.</td>
</tr>
<tr>
<td>attribute-map map-name</td>
<td></td>
</tr>
<tr>
<td>Step 9 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 10 show ip bgp neighbors [advertised-routes]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 11 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
To delete an aggregate entry, use the **no aggregate-address address mask** router configuration command. To return options to the default values, use the command with keywords.

### Configuring Routing Domain Confederations

One way to reduce the IBGP mesh is to divide an autonomous system into multiple subautonomous systems and to group them into a single confederation that appears as a single autonomous system. Each autonomous system is fully meshed within itself and has a few connections to other autonomous systems in the same confederation. Even though the peers in different autonomous systems have EBGP sessions, they exchange routing information as if they were IBGP peers. Specifically, the next hop, MED, and local preference information is preserved. You can then use a single IGP for all of the autonomous systems.

To configure a BGP confederation, you must specify a confederation identifier that acts as the autonomous system number for the group of autonomous systems.

Beginning in privileged EXEC mode, use these commands to configure a BGP confederation:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router bgp autonomous-system</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>bgp confederation identifier autonomous-system</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bgp confederation peers autonomous-system [autonomous-system ...]</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show ip bgp neighbor</td>
</tr>
<tr>
<td></td>
<td>show ip bgp network</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

### Configuring BGP Route Reflectors

BGP requires that all of the IBGP speakers be fully meshed. When a router receives a route from an external neighbor, it must advertise it to all internal neighbors. To prevent a routing information loop, all IBGP speakers must be connected. The internal neighbors do not send routes learned from internal neighbors to other internal neighbors.

With route reflectors, all IBGP speakers need not be fully meshed because another method is used to pass learned routes to neighbors. When you configure an internal BGP peer to be a *route reflector*, it is responsible for passing IBGP learned routes to a set of IBGP neighbors. The internal peers of the route reflector are divided into two groups: *client peers* and *nonclient peers* (all the other routers in the autonomous system). A route reflector reflects routes between these two groups. The route reflector and its client peers form a *cluster*. The nonclient peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with IBGP speakers outside their cluster.
When the route reflector receives an advertised route, it takes one of these actions, depending on the neighbor:

- A route from an external BGP speaker is advertised to all clients and nonclient peers.
- A route from a nonclient peer is advertised to all clients.
- A route from a client is advertised to all clients and nonclient peers. Hence, the clients need not be fully meshed.

Usually a cluster of clients have a single route reflector, and the cluster is identified by the route reflector router ID. To increase redundancy and to avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the same 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. All the route reflectors serving a cluster should be fully meshed and should have identical sets of client and nonclient peers.

Beginning in privileged EXEC mode, use these commands to configure a route reflector and clients:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router bgp autonomous-system</code> Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>`neighbor ip-address</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>bgp cluster-id cluster-id</code> (Optional) Configure the cluster ID if the cluster has more than one route reflector.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>no bgp client-to-client reflection</code> (Optional) Disable client-to-client route reflection. By default, the routes from a route reflector client are reflected to other clients. However, if the clients are fully meshed, the route reflector does not need to reflect routes to clients.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>show ip bgp</code> Verify the configuration. Display the originator ID and the cluster-list attributes.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

## Configuring Route Dampening

Route flap dampening is a BGP feature designed to minimize the propagation of flapping routes across an internetwork. A route is considered to be flapping when it is repeatedly available, then unavailable, then available, then unavailable, and so on. When route dampening is enabled, a numeric penalty value is assigned to a route when it flaps. When a route’s accumulated penalties reach a configurable limit, BGP suppresses advertisements of the route, even if the route is running. The reuse limit is a configurable value that is compared with the penalty. If the penalty is less than the reuse limit, a suppressed route that is up is advertised again.

Dampening is not applied to routes that are learned by IBGP. This policy prevents the IBGP peers from having a higher penalty for routes external to the AS.
Beginning in privileged EXEC mode, use these commands to configure BGP route dampening:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>router bgp autonomous-system</td>
<td>Enter BGP router configuration mode.</td>
</tr>
<tr>
<td>bgp dampening</td>
<td>Enable BGP route dampening.</td>
</tr>
<tr>
<td>bgp dampening half-life reuse suppress max-suppress [route-map map]</td>
<td>(Optional) Change the default values of route dampening factors.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip bgp flap-statistics [{regexp regexp}</td>
<td>(Optional) Monitor the flaps of all paths that are flapping. The statistics are deleted when the route is not suppressed and is stable.</td>
</tr>
<tr>
<td>filter-list list]</td>
<td></td>
</tr>
<tr>
<td>address mask [longer-prefix]]</td>
<td></td>
</tr>
<tr>
<td>show ip bgp dampened-paths</td>
<td>(Optional) Display the dampened routes, including the time remaining before they are suppressed.</td>
</tr>
<tr>
<td>clear ip bgp flap-statistics [{regexp regexp}</td>
<td>(Optional) Clear BGP flap statistics to make it less likely that a route will be dampened.</td>
</tr>
<tr>
<td>filter-list list]</td>
<td></td>
</tr>
<tr>
<td>address mask [longer-prefix]]</td>
<td></td>
</tr>
<tr>
<td>clear ip bgp dampening</td>
<td>(Optional) Clear route dampening information, and unsuppress the suppressed routes.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable flap dampening, use the no bgp dampening router configuration command without keywords. To set dampening factors back to the default values, use the no bgp dampening router configuration command with values.

### Monitoring and Maintaining BGP

You can remove all contents of a particular cache, table, or database. This might be necessary when the contents of the particular structure have become or are suspected to be invalid.

You can display specific statistics, such as the contents of BGP routing tables, caches, and databases. You can use the information to get resource utilization and solve network problems. You can also display information about node reachability and discover the routing path your device’s packets are taking through the network.

Table 37-8 lists the privileged EXEC commands for clearing and displaying BGP. For explanations of the display fields, see the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip bgp address</td>
<td>Reset a particular BGP connection.</td>
</tr>
<tr>
<td>clear ip bgp *</td>
<td>Reset all BGP connections.</td>
</tr>
<tr>
<td>clear ip bgp peer-group tag</td>
<td>Remove all members of a BGP peer group.</td>
</tr>
</tbody>
</table>
Configuring ISO CLNS Routing

The International Organization for Standardization (ISO) Connectionless Network Service (CLNS) protocol is a standard for the network layer of the Open System Interconnection (OSI) model. Addresses in the ISO network architecture are referred to as network service access point (NSAP) addresses and network entity titles (NETs). Each node in an OSI network has one or more NETs. In addition, each node has many NSAP addresses.

When you enable connectionless routing on the switch by using the clns routing global configuration command, the switch makes only forwarding decisions, with no routing-related functionality. For dynamic routing, you must also enable a routing protocol. The switch supports the Intermediate System-to-Intermediate System (IS-IS) dynamic routing protocol that is based on the OSI routing protocol for ISO CLNS networks.

You can also enable the logging of messages generated when a BGP neighbor resets, comes up, or goes down by using the bgp log-neighbor changes router configuration command.

### Configuring ISO CLNS Routing

Table 37-11  IP BGP Clear and Show Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp prefix</td>
<td>Display peer groups and peers not in peer groups to which the prefix has been advertised. Also display prefix attributes such as the next hop and the local prefix.</td>
</tr>
<tr>
<td>show ip bgp cidr-only</td>
<td>Display all BGP routes that contain subnet and supernet network masks.</td>
</tr>
<tr>
<td>show ip bgp community [community-number] [exact]</td>
<td>Display routes that belong to the specified communities.</td>
</tr>
<tr>
<td>show ip bgp community-list community-list-number [exact-match]</td>
<td>Display routes that are permitted by the community list.</td>
</tr>
<tr>
<td>show ip bgp filter-list access-list-number</td>
<td>Display routes that are matched by the specified AS path access list.</td>
</tr>
<tr>
<td>show ip bgp inconsistent-as</td>
<td>Display the routes with inconsistent originating autonomous systems.</td>
</tr>
<tr>
<td>show ip bgp regexp regular-expression</td>
<td>Display the routes that have an AS path that matches the specified regular expression entered on the command line.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Display the contents of the BGP routing table.</td>
</tr>
<tr>
<td>show ip bgp neighbors [address]</td>
<td>Display detailed information on the BGP and TCP connections to individual neighbors.</td>
</tr>
<tr>
<td>show ip bgp neighbors [address] [advertised-routes</td>
<td>Display routes learned from a particular BGP neighbor.</td>
</tr>
<tr>
<td>dampened-routes</td>
<td>flap-statistics</td>
</tr>
<tr>
<td>show ip bgp paths</td>
<td>Display all BGP paths in the database.</td>
</tr>
<tr>
<td>show ip bgp peer-group [tag] [summary]</td>
<td>Display information about BGP peer groups.</td>
</tr>
<tr>
<td>show ip bgp summary</td>
<td>Display the status of all BGP connections.</td>
</tr>
</tbody>
</table>
When dynamically routing, you use IS-IS. This routing protocol supports the concept of *areas*. Within an area, all routers know how to reach all the system IDs. Between areas, routers know how to reach the proper area. IS-IS supports two levels of routing: *station routing* (within an area) and *area routing* (between areas).

The key difference between the ISO IGRP and IS-IS NSAP addressing schemes is in the definition of area addresses. Both use the system ID for Level 1 routing (routing within an area). However, they differ in the way addresses are specified for area routing. An ISO IGRP NSAP address includes three separate fields for routing: the *domain*, *area*, and *system ID*. An IS-IS address includes two fields: a single continuous *area* field (comprising the domain and area fields) and the *system ID*.

**Note**

For more detailed information about ISO CLNS, see the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Configuration Guide, Release 12.2*. For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2*, use the IOS command reference master index, or search online.

### Configuring IS-IS Dynamic Routing

IS-IS is an ISO dynamic routing protocol (described in ISO 105890). Unlike other routing protocols, enabling IS-IS requires that you create an IS-IS routing process and assign it to a specific interface, rather than to a network. You can specify more than one IS-IS routing process per Layer 3 switch or router by using the multiarea IS-IS configuration syntax. You then configure the parameters for each instance of the IS-IS routing process.

Small IS-IS networks are built as a single area that includes all the routers in the network. As the network grows larger, it is usually reorganized into a backbone area made up of the connected set of all Level 2 routers from all areas, which is in turn connected to local areas. Within a local area, routers know how to reach all system IDs. Between areas, routers know how to reach the backbone, and the backbone routers know how to reach other areas.

Routers establish Level 1 adjacencies to perform routing within a local area (station routing). Routers establish Level 2 adjacencies to perform routing between Level 1 areas (area routing).

A single Cisco router can participate in routing in up to 29 areas and can perform Level 2 routing in the backbone. In general, each routing process corresponds to an area. By default, the first instance of the routing process configured performs both Level 1 and Level 2 routing. You can configure additional router instances, which are automatically treated as Level 1 areas. You must configure the parameters for each instance of the IS-IS routing process individually.

For IS-IS multiarea routing, you can configure only one process to perform Level 2 routing, although you can define up to 29 Level 1 areas for each Cisco unit. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform Level 1 routing at the same time. If Level 2 routing is not desired for a router instance, remove the Level 2 capability using the *is-type* global configuration command. Use the *is-type* command also to configure a different router instance as a Level 2 router.

**Note**

For more detailed information about IS-IS, see the “IP Routing Protocols” chapter of the *Cisco IOS IP Configuration Guide, Release 12.2*. For complete syntax and usage information for the commands used in this section, see the *Cisco IOS IP Command Reference, Release 12.2*. 
This section briefly describes how to configure IS-IS routing. It includes this information:

- Default IS-IS Configuration, page 37-64
- Enabling IS-IS Routing, page 37-65
- Configuring IS-IS Global Parameters, page 37-67
- Configuring IS-IS Interface Parameters, page 37-69

## Default IS-IS Configuration

Table 37-12 shows the default IS-IS configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore link-state PDU (LSP) errors</td>
<td>Enabled.</td>
</tr>
</tbody>
</table>
| IS-IS type                                   | Conventional IS-IS: the router acts as both a Level 1 (station) and a Level 2 (area) router.  
 |                                              | Multiarea IS-IS: the first instance of the IS-IS routing process is a Level 1-2 router. Remaining instances are Level 1 routers. |
| Default-information originate                | Disabled.                                                                       |
| Log IS-IS adjacency state changes.           | Disabled.                                                                       |
| LSP generation throttling timers             | Maximum interval between two consecutive occurrences: 5 seconds.               |
|                                              | Initial LSP generation delay: 50 ms.                                             |
|                                              | Hold time between the first and second LSP generation: 5000 ms.                 |
| LSP maximum lifetime (without a refresh)     | 1200 seconds (20 minutes) before the LSP packet is deleted.                     |
| LSP refresh interval                         | Send LSP refreshes every 900 seconds (15 minutes).                              |
| Maximum LSP packet size                      | 1497 bytes.                                                                    |
| NSF Awareness\(^1\) (Cisco IOS Release 12.2(25)SEG or later) | Enabled. Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware or software changes. |
| Partial route computation (PRC) throttling timers | Maximum PRC wait interval: 5 seconds.                                           |
|                                              | Initial PRC calculation delay after a topology change: 2000 ms.                |
|                                              | Hold time between the first and second PRC calculation: 5000 ms.               |
| Partition avoidance                          | Disabled.                                                                       |
| Password                                     | No area or domain password is defined, and authentication is disabled.          |
| Set-overload-bit                             | Disabled. When enabled, if no arguments are entered, the overload bit is set immediately and remains set until you enter the no set-overload-bit command. |
| Shortest path first (SPF) throttling timers  | Maximum interval between consecutive SFPs: 10 seconds.                          |
|                                              | Initial SPF calculation after a topology change: 5500 ms.                       |
|                                              | Hold time between the first and second SPF calculation: 5500 ms.               |
| Summary-address                              | Disabled.                                                                       |

\(^1\) NSF = Nonstop forwarding.
### Nonstop Forwarding Awareness

The integrated IS-IS NSF Awareness feature is supported for IPv4. The feature allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. The local router is not necessarily performing NSF, but its awareness of NSF allows the integrity and accuracy of the routing database and link-state database on the neighboring NSF-capable router to be maintained during the switchover process.

This feature is automatically enabled and requires no configuration. For more information on this feature, see the Integrated IS-IS Nonstop Forwarding (NSF) Awareness Feature Guide: [http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/isnsfawa.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/isnsfawa.html)

### Enabling IS-IS Routing

To enable IS-IS, you specify a name and NET for each routing process. You then enable IS-IS routing on the interface and specify the area for each instance of the routing process.

Beginning in privileged EXEC mode, follow these steps to enable IS-IS and specify the area for each instance of the IS-IS routing process:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>clns routing</td>
<td>Enable ISO connectionless routing on the switch.</td>
</tr>
<tr>
<td>3</td>
<td>router isis [area tag]</td>
<td>Enable the IS-IS routing for the specified routing process and enter IS-IS routing configuration mode. (Optional) Use the area tag argument to identify the area to which the IS-IS router is assigned. You must enter a value if you are configuring multiple IS-IS areas. The first IS-IS instance configured is Level 1-2 by default. Later instances are automatically Level 1. You can change the level of routing by using the is-type global configuration command.</td>
</tr>
<tr>
<td>4</td>
<td>net network-entity-title</td>
<td>Configure the NETs for the routing process. If you are configuring multiarea IS-IS, specify a NET for each routing process. You can specify a name for a NET and for an address.</td>
</tr>
</tbody>
</table>
| 5     | is-type {level-1 | level-1-2 | level-2-only} | (Optional) You can configure the router to act as a Level 1 (station) router, a Level 2 (area) router for multi-area routing, or both (the default):  
  - level-1—act as a station router only  
  - level-1-2—act as both a station router and an area router  
  - level 2—act as an area router only |
| 6     | exit | Return to global configuration mode. |
| 7     | interface interface-id | Specify an interface to route IS-IS, and enter interface configuration mode. If the interface is not already configured as a Layer 3 interface, enter the no switchport command to put it into Layer 3 mode. |
| 8     | ip router isis [area tag] | Configure an IS-IS routing process for ISO CLNS on the interface and attach an area designator to the routing process. |
| 9     | clns router isis [area tag] | Enable ISO CLNS on the interface. |
## Configuring ISO CLNS Routing

### Step 10
`ip address ip-address-mask`
Define the IP address for the interface. An IP address is required on all interfaces in an area enabled for IS-IS if any one interface is configured for IS-IS routing.

### Step 11
`end`
Return to privileged EXEC mode.

### Step 12
`show isis [area tag] database detail`
Verify your entries.

### Step 13
`copy running-config startup-config`
(Optional) Save your entries in the configuration file.

To disable IS-IS routing, use the `no router isis area-tag` router configuration command.

This example shows how to configure three routers to run conventional IS-IS as an IP routing protocol. In conventional IS-IS, all routers act as Level 1 and Level 2 routers (by default).

### Router A
```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000a.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

### Router B
```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000b.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```

### Router C
```
Switch(config)# clns routing
Switch(config)# router isis
Switch(config-router)# net 49.0001.0000.0000.000c.00
Switch(config-router)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip router isis
Switch(config-if)# clns router isis
Switch(config-router)# exit
```
Configuring IS-IS Global Parameters

These are some optional IS-IS global parameters that you can configure:

- You can force a default route into an IS-IS routing domain by configuring a default route controlled by a route map. You can also specify other filtering options configurable under a route map.
- You can configure the router to ignore IS-IS LSPs that are received with internal checksum errors or to purge corrupted LSPs, which causes the initiator of the LSP to regenerate it.
- You can assign passwords to areas and domains.
- You can create aggregate addresses that are represented in the routing table by a summary address (route-summarization). Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the specific routes.
- You can set an overload bit.
- You can configure the router to ignore IS-IS LSPs that are received with internal checksum errors, instead of purging the corrupted LSPs. To purge the corrupted LSPs, enter the no ignore-lsp-errors router configuration command.
- You can configure the switch to generate a log message when an IS-IS adjacency changes state (up or down).
- If a link in the network has a maximum transmission unit (MTU) size of less than 1500 bytes, you can lower the LSP MTU so that routing will still occur.
- The partition avoidance router configuration command prevents an area from becoming partitioned when full connectivity is lost among a Level1-2 border router, adjacent Level 1 routers, and end hosts.

Beginning in privileged EXEC mode, follow these steps to configure IS-IS parameters:

<table>
<thead>
<tr>
<th>Command</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> clns routing</td>
<td>Enable ISO connectionless routing on the switch.</td>
</tr>
<tr>
<td><strong>Step 3</strong> router isis</td>
<td>Specify the IS-IS routing protocol and enter router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> default-information originate</td>
<td>(Optional) Force a default route into the IS-IS routing domain. If you enter route-map map-name, the routing process generates the default route if the route map is satisfied.</td>
</tr>
<tr>
<td>[route-map map-name]</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ignore-lsp-errors</td>
<td>(Optional) Configure the router to ignore LSPs with internal checksum errors, instead of purging the LSPs. This command is enabled by default (corrupted LSPs are dropped). To purge the corrupted LSPs, enter the no ignore-lsp-errors router configuration command.</td>
</tr>
<tr>
<td><strong>Step 6</strong> area-password password</td>
<td>(Optional) Configure the area authentication password, which is inserted in Level 1 (station router level) LSPs.</td>
</tr>
<tr>
<td><strong>Step 7</strong> domain-password password</td>
<td>(Optional) Configure the routing domain authentication password, which is inserted in Level 2 (area router level) LSPs.</td>
</tr>
<tr>
<td><strong>Step 8</strong> summary-address address mask</td>
<td>(Optional) Create a summary of addresses for a given level.</td>
</tr>
<tr>
<td>[level-1</td>
<td>level-1-2</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 9** set-overload-bit [on-startup [seconds | (Optional) Set an overload bit (a hippity bit) to allow other routers to ignore the router in their shortest path first (SPF) calculations if the router is having problems.  
- (Optional) **on-startup**—sets the overload bit only on startup. If **on-startup** is not specified, the overload bit is set immediately and remains set until you enter the **no set-overload-bit** command. If **on-startup** is specified, you must enter a number of seconds or **wait-for-bgp**.  
- **seconds**—When the **on-startup** keyword is configured, causes the overload bit to be set upon system startup and remain set for this number of seconds. The range is from 5 to 86400 seconds.  
- **wait-for-bgp**—When the **on-startup** keyword is configured, causes the overload bit to be set upon system startup and remain set until BGP has converged. If BGP does not signal IS-IS that it is converged, IS-IS will turn off the overload bit after 10 minutes.
|  
| **Step 10** lsp-refresh-interval seconds | (Optional) Set an LSP refresh interval in seconds. The range is from 1 to 65535 seconds. The default is to send LSP refreshes every 900 seconds (15 minutes). |
| **Step 11** max-lsp-lifetime seconds | (Optional) Set the maximum time that LSP packets remain in the router database without being refreshed. The range is from 1 to 65535 seconds. The default is 1200 seconds (20 minutes). After the specified time interval, the LSP packet is deleted. |
| **Step 12** lsp-gen-interval [level-1 | (Optional) Set the IS-IS LSP generation throttling timers:  
- **lsp-max-wait**—the maximum interval (in seconds) between two consecutive occurrences of an LSP being generated. The range is 1 to 120, the default is 5.  
- **lsp-initial-wait**—the initial LSP generation delay (in milliseconds). The range is 1 to 10000; the default is 50.  
- **lsp-second-wait**—the hold time between the first and second LSP generation (in milliseconds). The range is 1 to 10000; the default is 5000. |
|  
| **Step 13** spf-interval [level-1 | (Optional) Sets IS-IS shortest path first (SPF) throttling timers.  
- **spf-max-wait**—the maximum interval between consecutive SPF (in seconds). The range is 1 to 120, the default is 10.  
- **spf-initial-wait**—the initial SPF calculation after a topology change (in milliseconds). The range is 1 to 10000; the default is 5500.  
- **spf-second-wait**—the holdtime between the first and second SPF calculation (in milliseconds). The range is 1 to 10000; the default is 5500. |
Chapter 37      Configuring IP Unicast Routing

Configuring IS-IS CLNS Routing

To disable default route generation, use the no default-information originate router configuration command. Use the no area-password or no domain-password router configuration command to disable passwords. To disable LSP MTU settings, use the no lsp mtu router configuration command. To return to the default conditions for summary addressing, LSP refresh interval, LSP lifetime, LSP timers, SFP timers, and PRC timers, use the no form of the commands. Use the no partition avoidance router configuration command to disable the output format.

Configuring IS-IS Interface Parameters

You can optionally configure certain interface-specific IS-IS parameters, independently from other attached routers. However, if you change some values from the defaults, such as multipliers and time intervals, it makes sense to also change them on multiple routers and interfaces. Most of the interface parameters can be configured for level 1, level 2, or both.

These are some interface level parameters you can configure:

- The default metric on the interface, which is used as a value for the IS-IS metric and assigned when there is no quality of service (QoS) routing performed.

- The hello interval (length of time between hello packets sent on the interface) or the default hello packet multiplier used on the interface to determine the hold time sent in IS-IS hello packets. The hold time determines how long a neighbor waits for another hello packet before declaring the neighbor down. This determines how quickly a failed link or neighbor is detected so that routes can be recalculated. Change the hello-multiplier in circumstances where hello packets are lost.
frequently and IS-IS adjacencies are failing unnecessarily. You can raise the hello multiplier and lower the hello interval correspondingly to make the hello protocol more reliable without increasing the time required to detect a link failure.

- **Other time intervals:**
  - Complete sequence number PDU (CSNP) interval. CSNPs are sent by the designated router to maintain database synchronization
  - Retransmission interval. This is the time between retransmission of IS-IS LSPs for point-to-point links.
  - IS-IS LSP retransmission throttle interval. This is the maximum rate (number of milliseconds between packets) at which IS-IS LSPs are re-sent on point-to-point links. This interval is different from the retransmission interval, which is the time between successive retransmissions of the same LSP

- Designated router election priority, which allows you to reduce the number of adjacencies required on a multiaccess network, which in turn reduces the amount of routing protocol traffic and the size of the topology database.

- The interface circuit type, which is the type of adjacency desired for neighbors on the specified interface

- Password authentication for the interface

Beginning in privileged EXEC mode, follow these steps to configure IS-IS interface parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>isis metric default-metric [level-1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>isis hello-interval {seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>isis hello-multiplier multiplier [level-1</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>isis csnp-interval seconds [level-1</td>
</tr>
</tbody>
</table>
## Monitoring and Maintaining ISO IGRP and IS-IS

You can remove all contents of a CLNS cache or remove information for a particular neighbor or route. You can display specific CLNS or IS-IS statistics, such as the contents of routing tables, caches, and databases. You can also display information about specific interfaces, filters, or neighbors.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td><strong>isis retransmit-interval seconds</strong></td>
</tr>
<tr>
<td>Step 8</td>
<td><strong>isis retransmit-throttle-interval milliseconds</strong></td>
</tr>
<tr>
<td>Step 9</td>
<td>**isis priority value [level-1</td>
</tr>
<tr>
<td>Step 10</td>
<td>**isis circuit-type {level-1</td>
</tr>
<tr>
<td></td>
<td>• <strong>level-1</strong>—a Level 1 adjacency is established if there is at least one area address common to both this node and its neighbors.</td>
</tr>
<tr>
<td></td>
<td>• <strong>level-1-2</strong>—a Level 1 and 2 adjacency is established if the neighbor is also configured as both Level 1 and Level 2 and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>level 2</strong>—a Level 2 adjacency is established. If the neighbor router is a Level 1 router, no adjacency is established.</td>
</tr>
<tr>
<td>Step 11</td>
<td>**isis password password [level-1</td>
</tr>
<tr>
<td>Step 12</td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Step 13</td>
<td><strong>show clns interface interface-id</strong></td>
</tr>
<tr>
<td>Step 14</td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>

To return to the default settings, use the **no** forms of the commands.
Table 37-13 lists the privileged EXEC commands for clearing and displaying ISO CLNS and IS-IS routing. For explanations of the display fields, see the Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS and XNS Command Reference, Release 12.2, use the Cisco IOS command reference master index, or search online.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear clns cache</td>
<td>Clear and reinitialize the CLNS routing cache.</td>
</tr>
<tr>
<td>clear clns es-neighbors</td>
<td>Remove end system (ES) neighbor information from the adjacency database.</td>
</tr>
<tr>
<td>clear clns is-neighbors</td>
<td>Remove intermediate system (IS) neighbor information from the adjacency database.</td>
</tr>
<tr>
<td>clear clns neighbors</td>
<td>Remove CLNS neighbor information from the adjacency database.</td>
</tr>
<tr>
<td>clear clns route</td>
<td>Remove dynamically derived CLNS routing information.</td>
</tr>
<tr>
<td>show clns</td>
<td>Display information about the CLNS network.</td>
</tr>
<tr>
<td>show clns cache</td>
<td>Display the entries in the CLNS routing cache.</td>
</tr>
<tr>
<td>show clns es-neighbors</td>
<td>Display ES neighbor entries, including the associated areas.</td>
</tr>
<tr>
<td>show clns filter-expr</td>
<td>Display filter expressions.</td>
</tr>
<tr>
<td>show clns filter-set</td>
<td>Display filter sets.</td>
</tr>
<tr>
<td>show clns interface</td>
<td>Display the CLNS-specific or ES-IS information about each interface.</td>
</tr>
<tr>
<td>show clns neighbor</td>
<td>Display information about IS-IS neighbors.</td>
</tr>
<tr>
<td>show clns protocol</td>
<td>List the protocol-specific information for each IS-IS or ISO IGRP routing process in this router.</td>
</tr>
<tr>
<td>show clns route</td>
<td>Display all the destinations to which this router knows how to route CLNS packets.</td>
</tr>
<tr>
<td>show clns traffic</td>
<td>Display information about the CLNS packets this router has seen.</td>
</tr>
<tr>
<td>show ip route isis</td>
<td>Display the current state of the ISIS IP routing table.</td>
</tr>
<tr>
<td>show isis database</td>
<td>Display the IS-IS link-state database.</td>
</tr>
<tr>
<td>show isis routes</td>
<td>Display the IS-IS Level 1 routing table.</td>
</tr>
<tr>
<td>show isis spf-log</td>
<td>Display a history of the shortest path first (SPF) calculations for IS-IS.</td>
</tr>
<tr>
<td>show isis topology</td>
<td>Display a list of all connected routers in all areas.</td>
</tr>
<tr>
<td>show route-map</td>
<td>Display all route maps configured or only the one specified.</td>
</tr>
<tr>
<td>trace clns destination</td>
<td>Discover the paths taken to a specified destination by packets in the network.</td>
</tr>
<tr>
<td>which-route [nsap-address</td>
<td>Display the routing table in which the specified CLNS destination is found.</td>
</tr>
<tr>
<td>\ clns-name]</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Multi-VRF CE

Virtual Private Networks (VPNs) provide a secure way for customers to share bandwidth over an ISP backbone network. A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service-provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table, called a VPN routing/forwarding (VRF) table.
The Catalyst 3560 switch supports multiple VPN routing/forwarding (multi-VRF) instances in customer edge (CE) devices (multi-VRF CE) when the switch is running the IP services image. Multi-VRF CE allows a service provider to support two or more VPNs with overlapping IP addresses. If you try to configure it on a switch running the IP base image, you see an error message. On a switch running the IP base image, configuring multi-VRF-CE and EIGRP stub routing at the same time is not allowed.

**Note**

The switch does not use Multiprotocol Label Switching (MPLS) to support VPNs. For information about MPLS VRF, refer to the *Cisco IOS Switching Services Configuration Guide, Release 12.2* from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

- Understanding Multi-VRF CE, page 37-73
- Default Multi-VRF CE Configuration, page 37-75
- Multi-VRF CE Configuration Guidelines, page 37-75
- Configuring VRFs, page 37-76
- Configuring VRF-Aware Services, page 37-78
- Configuring a VPN Routing Session, page 37-82
- Configuring BGP PE to CE Routing Sessions, page 37-82
- Multi-VRF CE Configuration Example, page 37-83
- Displaying Multi-VRF CE Status, page 37-87

**Understanding Multi-VRF CE**

Multi-VRF CE is a feature that allows a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. Multi-VRF CE uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but an interface cannot belong to more than one VRF at any time.

**Note**

Multi-VRF CE interfaces must be Layer 3 interfaces.

Multi-VRF CE includes these devices:

- Customer edge (CE) devices provide customers access to the service-provider network over a data link to one or more provider edge routers. The CE device advertises the site’s local routes to the router and learns the remote VPN routes from it. The Catalyst 3560 switch can be a CE.

- Provider edge (PE) routers exchange routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv2, OSPF, or EIGRP. The PE is only required to maintain VPN routes for those VPNs to which it is directly attached, eliminating the need for the PE to maintain all of the service-provider VPN routes. Each PE router maintains a VRF for each of its directly connected sites. Multiple interfaces on a PE router can be associated with a single VRF if all of these sites participate in the same VPN. Each VPN is mapped to a specified VRF. After learning local VPN routes from CEs, a PE router exchanges VPN routing information with other PE routers by using internal BGP (IBPG).

- Provider routers or core routers are any routers in the service provider network that do not attach to CE devices.
With multi-VRF CE, multiple customers can share one CE, and only one physical link is used between the CE and the PE. The shared CE maintains separate VRF tables for each customer and switches or routes packets for each customer based on its own routing table. Multi-VRF CE extends limited PE functionality to a CE device, giving it the ability to maintain separate VRF tables to extend the privacy and security of a VPN to the branch office.

Figure 37-6 shows a configuration using Catalyst 3560IE3000 switches as multiple virtual CEs. This scenario is suited for customers who have low bandwidth requirements for their VPN service, for example, small companies. In this case, multi-VRF CE support is required in the Catalyst 3560IE3000 switches. Because multi-VRF CE is a Layer 3 feature, each interface in a VRF must be a Layer 3 interface.

When the CE switch receives a command to add a Layer 3 interface to a VRF, it sets up the appropriate mapping between the VLAN ID and the policy label (PL) in multi-VRF-CE-related data structures and adds the VLAN ID and PL to the VLAN database.

When multi-VRF CE is configured, the Layer 3 forwarding table is conceptually partitioned into two sections:

- The multi-VRF CE routing section contains the routes from different VPNs.
- The global routing section contains routes to non-VPN networks, such as the Internet.

VLAN IDs from different VRFs are mapped into different policy labels, which are used to distinguish the VRFs during processing. For each new VPN route learned, the Layer 3 setup function retrieves the policy label by using the VLAN ID of the ingress port and inserts the policy label and new route to the multi-VRF CE routing section. If the packet is received from a routed port, the port internal VLAN ID number is used; if the packet is received from an SVI, the VLAN number is used.

This is the packet-forwarding process in a multi-VRF-CE-enabled network:

- When the switch receives a packet from a VPN, the switch looks up the routing table based on the input policy label number. When a route is found, the switch forwards the packet to the PE.
- When the ingress PE receives a packet from the CE, it performs a VRF lookup. When a route is found, the router adds a corresponding MPLS label to the packet and sends it to the MPLS network.
- When an egress PE receives a packet from the network, it strips the label and uses the label to identify the correct VPN routing table. Then it performs the normal route lookup. When a route is found, it forwards the packet to the correct adjacency.
- When a CE receives a packet from an egress PE, it uses the input policy label to look up the correct VPN routing table. If a route is found, it forwards the packet within the VPN.
To configure VRF, you create a VRF table and specify the Layer 3 interface associated with the VRF. Then configure the routing protocols in the VPN and between the CE and the PE. BGP is the preferred routing protocol used to distribute VPN routing information across the provider’s backbone. The multi-VRF CE network has three major components:

- VPN route target communities—lists of all other members of a VPN community. You need to configure VPN route targets for each VPN community member.
- Multiprotocol BGP peering of VPN community PE routers—propagates VRF reachability information to all members of a VPN community. You need to configure BGP peering in all PE routers within a VPN community.
- VPN forwarding—transports all traffic between all VPN community members across a VPN service-provider network.

**Default Multi-VRF CE Configuration**

Table 37-14 shows the default VRF configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Disabled. No VRFs are defined.</td>
</tr>
<tr>
<td>Maps</td>
<td>No import maps, export maps, or route maps are defined.</td>
</tr>
<tr>
<td>VRF maximum routes</td>
<td>Fast Ethernet switches: 8000.</td>
</tr>
</tbody>
</table>
<pre><code>                                    | Gigabit Ethernet switches: 12000.                    |
</code></pre>
<p>| Forwarding table       | The default for an interface is the global routing table. |</p>

**Multi-VRF CE Configuration Guidelines**

To use multi-VRF CE, you must have the IP services image installed on your switch.

These are considerations when configuring VRF in your network:

- A switch with multi-VRF CE is shared by multiple customers, and each customer has its own routing table.
- Because customers use different VRF tables, the same IP addresses can be re-used. Overlapped IP addresses are allowed in different VPNs.
- Multi-VRF CE lets multiple customers share the same physical link between the provider edge (PE) and the customer edge (CE). Trunk ports with multiple VLANs separate packets among customers. Each customer has its own VLAN.
- Multi-VRF CE does not support all MPLS-VRF functionality. It does not support label exchange, LDP adjacency, or labeled packets.
- For the PE router, there is no difference between using multi-VRF CE or using multiple CEs. In Figure 37-6, multiple virtual Layer 3 interfaces are connected to the multi-VRF CE device.
- The switch supports configuring VRF by using physical ports, VLAN SVIs, or a combination of both. The SVIs can be connected through an access port or a trunk port.
• A customer can use multiple VLANs as long as they do not overlap with those of other customers. A customer’s VLANs are mapped to a specific routing table ID that is used to identify the appropriate routing tables stored on the switch.
• A Catalyst 3560IE3000 switch supports one global network and up to 26 VRFs.
• Most routing protocols (BGP, OSPF, RIP, and static routing) can be used between the CE and the PE. However, we recommend using external BGP (EBGP) for these reasons:
  – BGP does not require multiple algorithms to communicate with multiple CEs.
  – BGP is designed for passing routing information between systems run by different administrations.
  – BGP makes it easy to pass attributes of the routes to the CE.
• Multi-VRF CE does not affect the packet switching rate.
• VPN multicast is not supported.
• Line-rate multicast forwarding within a multi-VRF CE is supported.
• A multicast VRF cannot coexist with private VLANs on the same interface.
• A maximum of 1000 multicast routes is supported and can be shared on all VRFs.
• If no VRFs are configured, 105 policies can be configured.
• If even one VRF is configured, 41 policies can be configured.
• If more than 41 policies are configured, VRF cannot be configured.
• VRF and private VLANs are mutually exclusive. You cannot enable VRF on a private VLAN. Similarly, you cannot enable a private VLAN on a VLAN with VRF configured on the VLAN interface.
• VRF and policy-based routing (PBR) are mutually exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface. The reverse is also true; you cannot enable PBR when VRF is enabled on an interface.
• VRF and Web Cache Communication Protocol (WCCP) are mutually exclusive on a switch interface. You cannot enable VRF when WCCP is enabled on an interface. The reverse is also true; you cannot enable WCCP when VRF is enabled on an interface.

**Configuring VRFs**

Beginning in privileged EXEC mode, follow these steps to configure one or more VRFs. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip routing</td>
<td>Enable IP routing.</td>
</tr>
<tr>
<td>3</td>
<td>ip vrf vrf-name</td>
<td>Name the VRF, and enter VRF configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>rd route-distinguisher</td>
<td>Create a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y)</td>
</tr>
</tbody>
</table>
Use the `no ip vrf vrf-name` global configuration command to delete a VRF and to remove all interfaces from it. Use the `no ip vrf forwarding` interface configuration command to remove an interface from the VRF.

## Configuring Multicast VRFs

Beginning in privileged EXEC mode, follow these steps to configure a multicast within a VRF table. For complete syntax and usage information for the commands, see the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2.*

<table>
<thead>
<tr>
<th>Command</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> ip routing</td>
<td>Enable IP routing mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ip vrf vrf-name</td>
<td>Name the VRF, and enter VRF configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> rd route-distinguisher</td>
<td>Create a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y).</td>
</tr>
<tr>
<td><strong>Step 5</strong> route-target { export</td>
<td>import</td>
</tr>
<tr>
<td><strong>Step 6</strong> import map route-map</td>
<td>(Optional) Associate a route map with the VRF.</td>
</tr>
<tr>
<td><strong>Step 7</strong> ip multicast-routing vrf vrf-name distributed</td>
<td>(Optional) Enable global multicast routing for VRF table.</td>
</tr>
<tr>
<td><strong>Step 8</strong> interface interface-id</td>
<td>Specify the Layer 3 interface to be associated with the VRF, and enter interface configuration mode. The interface can be a routed port or an SVI.</td>
</tr>
</tbody>
</table>
Configuring VRF-Aware Services

IP services can be configured on global interfaces, and these services run within the global routing instance. IP services are enhanced to run on multiple routing instances; they are VRF-aware. Any configured VRF in the system can be specified for a VRF-aware service.

VRF-Aware services are implemented in platform-independent modules. VRF means multiple routing instances in Cisco IOS. Each platform has its own limit on the number of VRFs it supports.

VRF-aware services have the following characteristics:

- The user can ping a host in a user-specified VRF.
- ARP entries are learned in separate VRFs. The user can display Address Resolution Protocol (ARP) entries for specific VRFs.

These services are VRF-Aware:

- ARP
- Ping
- Simple Network Management Protocol (SNMP)
- Hot Standby Router Protocol (HSRP)
- RADIUS
- Syslog
- Traceroute
- FTP and TFTP

Note: VRF-Aware services are not supported for Unicast Reverse Path Forwarding (uRPF).
**User Interface for ARP**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for ARP. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip arp vrf vrf-name</td>
<td>Display the ARP table in the specified VRF.</td>
</tr>
</tbody>
</table>

**User Interface for PING**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for ping. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping vrf vrf-name ip-host</td>
<td>Display the ARP table in the specified VRF.</td>
</tr>
</tbody>
</table>

**User Interface for SNMP**

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for SNMP. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>snmp-server trap authentication vrf</td>
<td>Enable SNMP traps for packets on a VRF.</td>
</tr>
<tr>
<td>3</td>
<td>snmp-server engineID remote &lt;host&gt; vrf &lt;vpn instance&gt; &lt;engine-id string&gt;</td>
<td>Configure a name for the remote SNMP engine on a switch.</td>
</tr>
<tr>
<td>4</td>
<td>snmp-server host &lt;host&gt; vrf &lt;vpn instance&gt; traps &lt;community&gt;</td>
<td>Specify the recipient of an SNMP trap operation and specify the VRF table to be used for sending SNMP traps.</td>
</tr>
<tr>
<td>5</td>
<td>snmp-server host &lt;host&gt; vrf &lt;vpn instance&gt; informs &lt;community&gt;</td>
<td>Specify the recipient of an SNMP inform operation and specify the VRF table to be used for sending SNMP informs.</td>
</tr>
<tr>
<td>6</td>
<td>snmp-server user &lt;user&gt; &lt;group&gt; remote &lt;host&gt; vrf &lt;vpn instance&gt; &lt;security model&gt;</td>
<td>Add a user to an SNMP group for a remote host on a VRF for SNMP access.</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
User Interface for HSRP

HSRP support for VRFs ensures that HSRP virtual IP addresses are added to the correct IP routing table. Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for HSRP. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the Cisco IOS Switching Services Command Reference, Release 12.2.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>no switchport</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip vrf forwarding &lt;vrf-name&gt;</td>
</tr>
<tr>
<td>Step 5</td>
<td>ip address ip address</td>
</tr>
<tr>
<td>Step 6</td>
<td>standby 1 ip ip address</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
</tbody>
</table>

User Interface for VRF-Aware RADIUS

To configure VRF-Aware RADIUS, you must first enable AAA on a RADIUS server. The switch supports the **ip vrf forwarding vrf-name** server-group configuration and the **ip radius source-interface** global configuration commands, as described in the Per VRF AAA Feature Guide: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html

User Interface for Syslog

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for Syslog. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the Cisco IOS Switching Services Command Reference, Release 12.2.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>logging on</td>
</tr>
<tr>
<td>Step 3</td>
<td>logging host ip address vrf vrf name</td>
</tr>
<tr>
<td>Step 4</td>
<td>logging buffered logging buffered size debugging</td>
</tr>
<tr>
<td>Step 5</td>
<td>logging trap debugging</td>
</tr>
<tr>
<td>Step 6</td>
<td>logging facility facility</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
</tbody>
</table>
User Interface for Traceroute

Beginning in privileged EXEC mode, follow these steps to configure VRF-aware services for traceroute. For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.2*.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>traceroute vrf vrf-name ipaddress</code></td>
<td>Specify the name of a VPN VRF in which to find the destination address.</td>
</tr>
</tbody>
</table>

User Interface for FTP and TFTP

So that FTP and TFTP are VRF-aware, you must configure some FTP/TFTP CLIs. For example, if you want to use a VRF table that is attached to an interface, say E1/0, you need to configure the CLI `ip [t]ftp source-interface E1/0` to inform [t]ftp to use a specific routing table. In this example, the VRF table is used to look up the destination IP address. These changes are backward-compatible and do not affect existing behavior. That is, you can use the source-interface CLI to send packets out a particular interface even if no VRF is configured on that interface.

To specify the source IP address for FTP connections, use the `ip ftp source-interface` show mode command. To use the address of the interface where the connection is made, use the `no` form of this command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>ip ftp source-interface interface-type interface-number</code></td>
<td>Specify the source IP address for FTP connections.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

To specify the IP address of an interface as the source address for TFTP connections, use the `ip tftp source-interface` show mode command. To return to the default, use the `no` form of this command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>ip tftp source-interface interface-type interface-number</code></td>
<td>Specify the source IP address for TFTP connections.</td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuring a VPN Routing Session

Routing within the VPN can be configured with any supported routing protocol (RIP, OSPF, EIGRP, or BGP) or with static routing. The configuration shown here is for OSPF, but the process is the same for other protocols.

**Note**

To configure an EIGRP routing process to run within a VRF instance, you must configure an autonomous-system number by entering the `autonomous-system autonomous-system-number` address-family configuration mode command.

Beginning in privileged EXEC mode, follow these steps to configure OSPF in the VPN:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id vrf vrf-name</td>
</tr>
<tr>
<td>Step 3</td>
<td>log-adjacency-changes</td>
</tr>
<tr>
<td>Step 4</td>
<td>redistribute bgp</td>
</tr>
<tr>
<td>Step 5</td>
<td>network network-number area area-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip ospf process-id</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the `no router ospf process-id vrf vrf-name` global configuration command to disassociate the VPN forwarding table from the OSPF routing process.

Configuring BGP PE to CE Routing Sessions

Beginning in privileged EXEC mode, follow these steps to configure a BGP PE to CE routing session:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>network network-number mask network-mask</td>
</tr>
<tr>
<td>Step 4</td>
<td>redistribute ospf process-id match internal</td>
</tr>
<tr>
<td>Step 5</td>
<td>network network-number area area-id</td>
</tr>
</tbody>
</table>
Use the `no router bgp autonomous-system-number` global configuration command to delete the BGP routing process. Use the command with keywords to delete routing characteristics.

### Multi-VRF CE Configuration Example

Figure 37-7 is a simplified example of the physical connections in a network similar to that in Figure 37-6. OSPF is the protocol used in VPN1, VPN2, and the global network. BGP is used in the CE to PE connections. The examples following the illustration show how to configure a Catalyst 3560IE3000 switch as CE Switch A, and the VRF configuration for customer switches D and F. Commands for configuring CE Switch C and the other customer switches are not included but would be similar. The example also includes commands for configuring traffic to Switch A for a Catalyst 6000 or Catalyst 6500 switch acting as a PE router.

#### Step 6

`address-family ipv4 vrf vrf-name`

Define BGP parameters for PE to CE routing sessions, and enter VRF address-family mode.

#### Step 7

`neighbor address remote-as as-number`

Define a BGP session between PE and CE routers.

#### Step 8

`neighbor address activate`

Activate the advertisement of the IPv4 address family.

#### Step 9

`end`

Return to privileged EXEC mode.

#### Step 10

`show ip bgp [ipv4] [neighbors]`

Verify BGP configuration.

#### Step 11

`copy running-config startup-config`

(Optional) Save your entries in the configuration file.

Use the `no router bgp autonomous-system-number` global configuration command to delete the BGP routing process. Use the command with keywords to delete routing characteristics.
Configuring Switch A

On Switch A, enable routing and configure VRF:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit

Configure the loopback and physical interfaces on Switch A. Gigabit Ethernet port 1 is a trunk connection to the PE. Fast Ethernet ports 8 and 11 connect to VPNs:

Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface gigabitethernet0/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface fastethernet0/11
Switch(config)# interface fastethernet0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Configure the VLANs used on Switch A. VLAN 10 is used by VRF 11 between the CE and the PE. VLAN 20 is used by VRF 12 between the CE and the PE. VLANs 118 and 208 are used for the VPNs that include Switch F and Switch D, respectively:

Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit

Configure OSPF routing in VPN1 and VPN2.
Switch(config)# router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit

Switch(config)# router ospf 2 vrf vl2
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit

Configure BGP for CE to PE routing.
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

Switch(config-router-af)# address-family ipv4 vrf vl1
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end

Configuring Switch D

Switch D belongs to VPN 1. Configure the connection to Switch A by using these commands.
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end

Configuring Switch F

Switch F belongs to VPN 2. Configure the connection to Switch A by using these commands.
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Configuring the PE Switch B

When used on switch B (the PE router), these commands configure only the connections to the CE device, Switch A.

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/0.10
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf v1
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end

Displaying Multi-VRF CE Status

You can use the privileged EXEC commands in Table 37-15 to display information about multi-VRF CE configuration and status.

**Table 37-15 Commands for Displaying Multi-VRF CE Information**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip protocols vrf vrf-name</td>
<td>Display routing protocol information associated with a VRF.</td>
</tr>
<tr>
<td>show ip route vrf vrf-name [connected] [protocol [as-number]] [list] [mobile] [odr] [profile] [static] [summary] [supernets-only]</td>
<td>Display IP routing table information associated with a VRF.</td>
</tr>
<tr>
<td>show ip vrf [brief</td>
<td>detail</td>
</tr>
</tbody>
</table>

For more information about the information in the displays, refer to the Cisco IOS Switching Services Command Reference, Release 12.2.

Configuring Protocol-Independent Features

This section describes how to configure IP routing protocol-independent features. These features are available on switches running the IP base image or the IP services image; except that with the IP base image, protocol-related features are available only for RIP. For a complete description of the IP routing protocol-independent commands in this chapter, see the “IP Routing Protocol-Independent Commands” chapter of the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

These sections contain this configuration information:

- Configuring Cisco Express Forwarding, page 37-88
- Configuring the Number of Equal-Cost Routing Paths, page 37-89
- Configuring Static Unicast Routes, page 37-89
- Specifying Default Routes and Networks, page 37-91
- Using Route Maps to Redistribute Routing Information, page 37-91
- Configuring Policy-Based Routing, page 37-95
- Filtering Routing Information, page 37-99
- Managing Authentication Keys, page 37-101
Configuring Cisco Express Forwarding

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology used to optimize network performance. CEF implements an advanced IP look-up and forwarding algorithm to deliver maximum Layer 3 switching performance. CEF is less CPU-intensive than fast switching route caching, allowing more CPU processing power to be dedicated to packet forwarding. In dynamic networks, fast switching cache entries are frequently invalidated because of routing changes, which can cause traffic to be processed switched using the routing table, instead of fast switched using the route cache. CEF uses the Forwarding Information Base (FIB) lookup table to perform destination-based switching of IP packets.

The two main components in CEF are the distributed FIB and the distributed adjacency tables.

- The FIB is similar to a routing table or information base and maintains a mirror image of the forwarding information in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because the FIB contains all known routes that exist in the routing table, CEF eliminates route cache maintenance, is more efficient for switching traffic, and is not affected by traffic patterns.

- Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.

Because the switch uses Application Specific Integrated Circuits (ASICs) to achieve Gigabit-speed line rate IP traffic, CEF forwarding applies only to the software-forwarding path, that is, traffic that is forwarded by the CPU.

CEF is enabled globally by default. If for some reason it is disabled, you can re-enable it by using the `ip cef` global configuration command.

The default configuration is CEF enabled on all Layer 3 interfaces. Entering the `no ip route-cache cef` interface configuration command disables CEF for traffic that is being forwarded by software. This command does not affect the hardware forwarding path. Disabling CEF and using the `debug ip packet detail` privileged EXEC command can be useful to debug software-forwarded traffic. To enable CEF on an interface for the software-forwarding path, use the `ip route-cache cef` interface configuration command.

![Caution]

Although the `no ip route-cache cef` interface configuration command to disable CEF on an interface is visible in the CLI, we strongly recommend that you do not disable CEF on interfaces except for debugging purposes.

Beginning in privileged EXEC mode, follow these steps to enable CEF globally and on an interface for software-forwarded traffic if it has been disabled:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip cef</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip route-cache cef</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
</tr>
<tr>
<td>Step 6</td>
<td>show ip cef</td>
</tr>
</tbody>
</table>
Configuring IP Unicast Routing

Configuring Protocol-Independent Features

Chapter 37  Configuring IP Unicast Routing

When a router has two or more routes to the same network with the same metrics, these routes can be thought of as having an equal cost. The term *parallel path* is another way to see occurrences of equal-cost routes in a routing table. If a router has two or more equal-cost paths to a network, it can use them concurrently. Parallel paths provide redundancy in case of a circuit failure and also enable a router to load balance packets over the available paths for more efficient use of available bandwidth.

Even though the router automatically learns about and configures equal-cost routes, you can control the maximum number of parallel paths supported by an IP routing protocol in its routing table. Although the switch software allows a maximum of 32 equal-cost routes, the switch hardware will never use more than 16 paths per route.

Beginning in privileged EXEC mode, follow these steps to change the maximum number of parallel paths installed in a routing table from the default:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>show cef linecard [detail]</code></td>
<td>Display CEF-related interface information.</td>
</tr>
<tr>
<td>8</td>
<td><code>show cef interface [interface-id]</code></td>
<td>Display detailed CEF information for all interfaces or the specified interface.</td>
</tr>
<tr>
<td>9</td>
<td><code>show adjacency</code></td>
<td>Display CEF adjacency table information.</td>
</tr>
<tr>
<td>10</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Configuring the Number of Equal-Cost Routing Paths

Use the `no maximum-paths` router configuration command to restore the default value.

### 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.
Beginning in privileged EXEC mode, follow these steps to configure a static route:

**Step 1**
configure terminal

Enter global configuration mode.

**Step 2**

ip route prefix mask {address | interface} [distance]

Establish a static route.

**Step 3**
end

Return to privileged EXEC mode.

**Step 4**
show ip route

Display the current state of the routing table to verify the configuration.

**Step 5**
copy running-config startup-config

(Optional) Save your entries in the configuration file.

Table 37-16 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>External BGP</td>
<td>20</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>Internal BGP</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>225</td>
</tr>
</tbody>
</table>

Use the no ip route prefix mask {address | interface} global configuration command to remove a static route.

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 37-16. 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.

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.
Specifying 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.

Beginning in privileged EXEC mode, follow these steps to define a static route to a network as the static default route:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip default-network network number Specify a default network.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip route Display the selected default route in the gateway of last resort display.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no ip default-network network number global configuration command to remove the route.

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.

Using Route Maps to Redistribute Routing Information

The switch can run multiple routing protocols simultaneously, and it can redistribute information from one routing protocol to another. Redistributing information from one routing protocol to another applies to all supported IP-based routing protocols.

You can also conditionally control the redistribution of routes between routing domains by defining enhanced packet filters or route maps between the two domains. The match and set route-map configuration commands define the condition portion of a route map. The match command specifies that a criterion must be matched. The set command specifies an action to be taken if the routing update meets
the conditions defined by the match command. Although redistribution is a protocol-independent feature, some of the match and set route-map configuration commands are specific to a particular protocol.

One or more match commands and one or more set commands follow a route-map command. If there are no match commands, everything matches. If there are no set commands, nothing is done, other than the match. Therefore, you need at least one match or set command.

Note

A route map with no set route-map configuration commands is sent to the CPU, which causes high CPU utilization.

You can also identify route-map statements as permit or deny. If the statement is marked as a deny, the packets meeting the match criteria are sent back through the normal forwarding channels (destination-based routing). If the statement is marked as permit, set clauses are applied to packets meeting the match criteria. Packets that do not meet the match criteria are forwarded through the normal routing channel.

You can use the BGP route map continue clause to execute additional entries in a route map after an entry is executed with successful match and set clauses. You can use the continue clause to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map. The switch supports the continue clause for outbound policies. For more information about using the route map continue clause, see the BGP Route-Map Continue Support for an Outbound Policy feature guide for Cisco IOS Release 12.4(4)T:

Note

Although each of Steps 3 through 14 in the following section is optional, you must enter at least one match route-map configuration command and one set route-map configuration command.

Beginning in privileged EXEC mode, follow these steps to configure a route map for redistribution:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>route-map map-tag [permit</td>
<td>deny] [sequence number]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>map-tag—A meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps might share the same map tag name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Optional) If permit is specified and the match criteria are met for this route map, the route is redistributed as controlled by the set actions. If deny is specified, the route is not redistributed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sequence number (Optional)— Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.</td>
</tr>
<tr>
<td>3</td>
<td>match as-path path-list-number</td>
<td>Match a BGP AS path access list.</td>
</tr>
<tr>
<td>4</td>
<td>match community-list community-list-number [exact]</td>
<td>Match a BGP community list.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>5</td>
<td>match ip address {access-list-number</td>
<td>access-list-name} [...access-list-number</td>
</tr>
<tr>
<td>6</td>
<td>match metric metric-value</td>
<td>Match the specified route metric. The <code>metric-value</code> can be an EIGRP metric with a specified value from 0 to 4294967295.</td>
</tr>
<tr>
<td>7</td>
<td>match ip next-hop {access-list-number</td>
<td>access-list-name} [...access-list-number</td>
</tr>
<tr>
<td>8</td>
<td>match tag tag-value [...tag-value]</td>
<td>Match the specified tag value in a list of one or more route tag values. Each can be an integer from 0 to 4294967295.</td>
</tr>
<tr>
<td>9</td>
<td>match interface type number [...type number]</td>
<td>Match the specified next hop route out one of the specified interfaces.</td>
</tr>
<tr>
<td>10</td>
<td>match ip route-source {access-list-number</td>
<td>access-list-name} [...access-list-number</td>
</tr>
</tbody>
</table>
| 11   | match route-type {local | internal | external [type-1 | type-2]} | Match the specified `route-type`:  
  - **local**—Locally generated BGP routes.  
  - **internal**—OSPF intra-area and interarea routes or EIGRP internal routes.  
  - **external**—OSPF external routes (Type 1 or Type 2) or EIGRP external routes. |
| 12   | set dampening halflife reuse suppress max-suppress-time | Set BGP route dampening factors. |
| 13   | set local-preference value | Assign a value to a local BGP path. |
| 14   | set origin {igp | egp as | incomplete} | Set the BGP origin code. |
| 15   | set as-path {tag | prepend as-path-string} | Modify the BGP autonomous system path. |
| 16   | set level {level-1 | level-2 | level-1-2 | stub-area | backbone} | Set the level for routes that are advertised into the specified area of the routing domain. The `stub-area` and `backbone` are OSPF NSSA and backbone areas. |
| 17   | set metric metric value | Set the metric value to give the redistributed routes (for EIGRP only). The `metric value` is an integer from -294967295 to 294967295. |
Chapter 37  Configuring IP Unicast Routing

### Configuring Protocol-Independent Features

To delete an entry, use the `no route-map map tag` global configuration command or the `no match` or `no set` route-map configuration commands.

You can distribute routes from one routing domain into another and control route distribution.

Beginning in privileged EXEC mode, follow these steps to control route redistribution. Note that the keywords are the same as defined in the previous procedure.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 18</strong></td>
<td><strong>set metric bandwidth delay reliability loading mtu</strong></td>
</tr>
<tr>
<td></td>
<td>Set the metric value to give the redistributed routes (for EIGRP only):</td>
</tr>
<tr>
<td></td>
<td>- <em>bandwidth</em>—Metric value or IGRP bandwidth of the route in kilobits per second in the range 0 to 4294967295</td>
</tr>
<tr>
<td></td>
<td>- <em>delay</em>—Route delay in tens of microseconds in the range 0 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td>- <em>reliability</em>—Likelihood of successful packet transmission expressed as a number between 0 and 255, where 255 means 100 percent reliability and 0 means no reliability.</td>
</tr>
<tr>
<td></td>
<td>- <em>loading</em>—Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).</td>
</tr>
<tr>
<td></td>
<td>- <em>mtu</em>—Minimum maximum transmission unit (MTU) size of the route in bytes in the range 0 to 4294967295.</td>
</tr>
<tr>
<td><strong>Step 19</strong></td>
<td>**set metric-type {type-1</td>
</tr>
<tr>
<td></td>
<td>Set the OSPF external metric type for redistributed routes.</td>
</tr>
<tr>
<td><strong>Step 20</strong></td>
<td><strong>set metric-type internal</strong></td>
</tr>
<tr>
<td></td>
<td>Set the multi-exit discriminator (MED) value on prefixes advertised to external BGP neighbor to match the IGP metric of the next hop.</td>
</tr>
<tr>
<td><strong>Step 21</strong></td>
<td><strong>set weight</strong></td>
</tr>
<tr>
<td></td>
<td>Set the BGP weight for the routing table. The value can be from 1 to 6535.</td>
</tr>
<tr>
<td><strong>Step 22</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 23</strong></td>
<td><strong>show route-map</strong></td>
</tr>
<tr>
<td></td>
<td>Display all route maps configured or only the one specified to verify configuration.</td>
</tr>
<tr>
<td><strong>Step 24</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To delete an entry, use the `no route-map map tag` global configuration command or the `no match` or `no set` route-map configuration commands.

You can distribute routes from one routing domain into another and control route distribution.

Beginning in privileged EXEC mode, follow these steps to control route redistribution. Note that the keywords are the same as defined in the previous procedure.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**router [bgp</td>
</tr>
<tr>
<td></td>
<td>Enter router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**redistribute protocol [process-id] [level-1</td>
</tr>
<tr>
<td></td>
<td>REDISTRIBUTE ROUTES FROM ONE ROUTING PROTOCOL TO ANOTHER. IF NO ROUTE-MAPS ARE SPECIFIED, ALL ROUTES ARE REDISTRIBUTED. IF THE KEYWORD <code>ROUTE-MAP</code> IS SPECIFIED WITH NO <code>MAP-TAG</code>, NO ROUTES ARE DISTRIBUTED.</td>
</tr>
</tbody>
</table>
To disable redistribution, use the `no` form of the commands.

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count, and the IGRP metric is a combination of five qualities. In these situations, an artificial metric is assigned to the redistributed route. Uncontrolled exchanging of routing information between different routing protocols can create routing loops and seriously degrade network operation.

If you have not defined a default redistribution metric that replaces metric conversion, some automatic metric translations occur between routing protocols:

- RIP can automatically redistribute static routes. It assigns static routes a metric of 1 (directly connected).
- Any protocol can redistribute other routing protocols if a default mode is in effect.

### Configuring Policy-Based Routing

You can use policy-based routing (PBR) to configure a defined policy for traffic flows. By using PBR, you can have more control over routing by reducing the reliance on routes derived from routing protocols. PBR can specify and implement routing policies that allow or deny paths based on:

- Identity of a particular end system
- Application
- Protocol

You can use PBR to provide equal-access and source-sensitive routing, routing based on interactive versus batch traffic, or routing based on dedicated links. For example, you could transfer stock records to a corporate office on a high-bandwidth, high-cost link for a short time while transmitting routine application data such as e-mail over a low-bandwidth, low-cost link.

With PBR, you classify traffic using access control lists (ACLs) and then make traffic go through a different path. PBR is applied to incoming packets. All packets received on an interface with PBR enabled are passed through route maps. Based on the criteria defined in the route maps, packets are forwarded (routed) to the appropriate next hop.

- If packets do not match any route map statements, all set clauses are applied.
- If a statement is marked as permit and the packets do not match any route-map statements, the packets are sent through the normal forwarding channels, and destination-based routing is performed.
- For PBR, route-map statements marked as deny are not supported.
For more information about configuring route maps, see the “Using Route Maps to Redistribute Routing Information” section on page 37-91.

You can use standard IP ACLs to specify match criteria for a source address or extended IP ACLs to specify match criteria based on an application, a protocol type, or an end station. The process proceeds through the route map until a match is found. If no match is found, normal destination-based routing occurs. There is an implicit deny at the end of the list of match statements.

If match clauses are satisfied, you can use a set clause to specify the IP addresses identifying the next hop router in the path.

For details about PBR commands and keywords, see the Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2. For a list of PBR commands that are visible but not supported by the switch, see Appendix C, “Unsupported Commands in Cisco IOS Release 12.2(55)SE.”

Note

This software release does not support PBR when processing IPv4 and IPv6 traffic.

PBR Configuration Guidelines

Before configuring PBR, you should be aware of this information:

- To use PBR, you must have the IP services image installed on the switch.
- Multicast traffic is not policy-routed. PBR applies to only to unicast traffic.
- You can enable PBR on a routed port or an SVI.
- The switch does not support route-map deny statements for PBR.
- You can apply a policy route map to an EtherChannel port channel in Layer 3 mode, but you cannot apply a policy route map to a physical interface that is a member of the EtherChannel. If you try to do so, the command is rejected. When a policy route map is applied to a physical interface, that interface cannot become a member of an EtherChannel.
- You can define a maximum of 246 IP policy route maps on the switch.
- You can define a maximum of 512 access control entries (ACEs) for PBR on the switch.
- When configuring match criteria in a route map, follow these guidelines:
  - Do not match ACLs that permit packets destined for a local address. PBR would forward these packets, which could cause ping or Telnet failure or route protocol flapping.
  - Do not match ACLs with deny ACEs. Packets that match a deny ACE are sent to the CPU, which could cause high CPU utilization.
- To use PBR, you must first enable the routing template by using the sdm prefer routing global configuration command. PBR is not supported with the VLAN or default template. For more information on the SDM templates, see Chapter 7, “Configuring SDM Templates.”
- VRF and PBR are mutually exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface. The reverse is also true, you cannot enable PBR when VRF is enabled on an interface.
- Web Cache Communication Protocol (WCCP) and PBR are mutually exclusive on a switch interface. You cannot enable WCCP when PBR is enabled on an interface. The reverse is also true, you cannot enable PBR when WCCP is enabled on an interface.
- The number of TCAM entries used by PBR depends on the route map itself, the ACLs used, and the order of the ACLs and route-map entries.
• Policy-based routing based on packet length, TOS, set interface, set default next hop, or set default interface are not supported. Policy maps with no valid set actions or with set action set to Don’t Fragment are not supported.

• The switch supports quality of service (QoS) DSCP and IP precedence matching in PBR route maps, with these limitations:
  – You cannot apply QoS DSCP mutation maps and PBR route maps to the same interface.
  – You cannot configure DSCP transparency and PBR DSCP route maps on the same switch.
  – When you configure PBR with QoS DSCP, you can set QoS to be enabled (by entering the mls qos global configuration command) or disabled (by entering the no mls qos command). When QoS is enabled, to ensure that the DSCP value of the traffic is unchanged, you should configure a DSCP trust state on the port where traffic enters the switch by entering the mls qos trust dscp interface configuration command. If the trust state is not DSCP, by default all nontrusted traffic would have the DSCP value marked as 0.

Enabling PBR

By default, PBR is disabled on the switch. To enable PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. Then, you must enable PBR for that route map on an interface. All packets arriving on the specified interface matching the match clauses are subject to PBR.

PBR can be fast-switched or implemented at speeds that do not slow down the switch. Fast-switched PBR supports most match and set commands. PBR must be enabled before you enable fast-switched PBR. Fast-switched PBR is disabled by default.

Packets that are generated by the switch, or local packets, are not normally policy-routed. When you globally enable local PBR on the switch, all packets that originate on the switch are subject to local PBR. Local PBR is disabled by default.

Note

To enable PBR, the switch must be running the IP services image.
Beginning in privileged EXEC mode, follow these steps to configure PBR:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>route-map map-tag [permit] [sequence number]</td>
<td>Define any route maps used to control where packets are output, and enter route-map configuration mode.</td>
</tr>
</tbody>
</table>

- **map-tag**—A meaningful name for the route map. The `ip policy route-map` interface configuration command uses this name to reference the route map. Multiple route maps might share the same map tag name.
- (Optional) If `permit` is specified and the match criteria are met for this route map, the route is policy-routed as controlled by the set actions.

**Note** The `route-map deny` statement is not supported in PBR route maps to be applied to an interface.

- **sequence number** (Optional)— Number that shows the position of a new route map in the list of route maps already configured with the same name.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>match ip address {access-list-number</td>
<td>Match the source and destination IP address that is permitted</td>
</tr>
<tr>
<td></td>
<td>access-list-name } [access-list-number</td>
<td>one or more standard or extended access lists.</td>
</tr>
<tr>
<td></td>
<td>...access-list-name]</td>
<td>Note: Do not enter an ACL with a deny ACE or an ACL that permits a packet destined for a local address.</td>
</tr>
</tbody>
</table>

If you do not specify a `match` command, the route map applies to all packets.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>set ip next-hop ip-address ...ip-address</td>
<td>Specify the action to take on the packets that match the criteria. Set next hop to which to route the packet (the next hop must be adjacent).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>ip policy route-map map-tag</td>
<td>Enable PBR on a Layer 3 interface, and identify the route map to use. You can configure only one route map on an interface. However, you can have multiple route map entries with different sequence number order until the first match. If there is no match, packets are routed as usual.</td>
</tr>
</tbody>
</table>

**Note** If the IP policy route map contains a `deny` statement, the configuration fails.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8</td>
<td>ip route-cache policy</td>
<td>(Optional) Enable fast-switching PBR. You must first enable PBR before enabling fast-switching PBR.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10</td>
<td>ip local policy route-map map-tag</td>
<td>(Optional) Enable local PBR to perform policy-based routing on packets originating at the switch. This applies to packets generated by the switch and not to incoming packets.</td>
</tr>
</tbody>
</table>
**Filtering Routing Information**

You can filter routing protocol information by performing the tasks described in this section.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 11 <code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 12 <code>show route-map [map-name]</code></td>
<td>(Optional) Display all route maps configured or only the one specified to verify configuration.</td>
</tr>
<tr>
<td>Step 13 <code>show ip policy</code></td>
<td>(Optional) Display policy route maps attached to interfaces.</td>
</tr>
<tr>
<td>Step 14 <code>show ip local policy</code></td>
<td>(Optional) Display whether or not local policy routing is enabled and, if so, the route map being used.</td>
</tr>
<tr>
<td>Step 15 <code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no route-map map-tag` global configuration command or the `no match` or `no set` route-map configuration commands to delete an entry. Use the `no ip policy route-map map-tag` interface configuration command to disable PBR on an interface. Use the `no ip route-cache policy` interface configuration command to disable fast-switching PBR. Use the `no ip local policy route-map map-tag` global configuration command to disable policy-based routing on packets originating on the switch.

**Setting Passive Interfaces**

To prevent other routers on a local network from dynamically learning about routes, you can use the `passive-interface` router configuration command to keep routing update messages from being sent through a router interface. When you use this command in the OSPF protocol, the interface address you specify as passive appears as a stub network in the OSPF domain. OSPF routing information is neither sent nor received through the specified router interface.

In networks with many interfaces, to avoid having to manually set them as passive, you can set all interfaces to be passive by default by using the `passive-interface default` router configuration command and manually setting interfaces where adjacencies are desired.

Beginning in privileged EXEC mode, follow these steps to configure passive interfaces:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 `router {bgp</td>
<td>rip</td>
</tr>
<tr>
<td>Step 3 <code>passive-interface interface-id</code></td>
<td>Suppress sending routing updates through the specified Layer 3 interface.</td>
</tr>
<tr>
<td>Step 4 <code>passive-interface default</code></td>
<td>(Optional) Set all interfaces as passive by default.</td>
</tr>
<tr>
<td>Step 5 <code>no passive-interface interface type</code></td>
<td>(Optional) Activate only those interfaces that need to have adjacencies sent.</td>
</tr>
<tr>
<td>Step 6 <code>network network-address</code></td>
<td>(Optional) Specify the list of networks for the routing process. The <code>network-address</code> is an IP address.</td>
</tr>
</tbody>
</table>

When routes are redistributed between OSPF processes, no OSPF metrics are preserved.
Chapter 37  Configuring IP Unicast Routing

Configuring Protocol-Independent Features

Use a network monitoring privileged EXEC command such as `show ip ospf interface` to verify the interfaces that you enabled as passive, or use the `show ip interface` privileged EXEC command to verify the interfaces that you enabled as active.

To re-enable the sending of routing updates, use the `no passive-interface interface-id` router configuration command. The `default` keyword sets all interfaces as passive by default. You can then configure individual interfaces where you want adjacencies by using the `no passive-interface` router configuration command. The `default` keyword is useful in Internet service provider and large enterprise networks where many of the distribution routers have more than 200 interfaces.

Controlling Advertising and Processing in Routing Updates

You can use the `distribute-list` router configuration command with access control lists to suppress routes from being advertised in routing updates and to prevent other routers from learning one or more routes. When used in OSPF, this feature applies to only external routes, and you cannot specify an interface name.

You can also use a `distribute-list` router configuration command to avoid processing certain routes listed in incoming updates. (This feature does not apply to OSPF.)

Beginning in privileged EXEC mode, follow these steps to control the advertising or processing of routing updates:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>`router {bgp</td>
</tr>
<tr>
<td>Step 3</td>
<td>`distribute-list {access-list-number</td>
</tr>
<tr>
<td>Step 4</td>
<td>`distribute-list {access-list-number</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the `no distribute-list in` router configuration command to change or cancel a filter. To cancel suppression of network advertisements in updates, use the `no distribute-list out` router configuration command.

Filtering Sources of Routing Information

Because some routing information might be more accurate than others, you can use filtering to prioritize information coming from different sources. An administrative distance is a rating of the trustworthiness of a routing information source, such as a router or group of routers. In a large network, some routing protocols can be more reliable than others. By specifying administrative distance values, you enable the router to intelligently discriminate between sources of routing information. The router always picks the
route whose routing protocol has the lowest administrative distance. Table 37-16 on page 37-90 shows the default administrative distances for various routing information sources.

Because each network has its own requirements, there are no general guidelines for assigning administrative distances.

Beginning in privileged EXEC mode, follow these steps to filter sources of routing information:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router {bgp</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>distance weight {ip-address {ip-address mask}} [ip access list]</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ip protocols</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove a distance definition, use the no distance router configuration command.

**Managing Authentication Keys**

Key management is a method of controlling authentication keys used by routing protocols. Not all protocols can use key management. Authentication keys are available for EIGRP and RIP Version 2.

Before you manage authentication keys, you must enable authentication. See the appropriate protocol section to see how to enable authentication for that protocol. To manage authentication keys, define a key chain, identify the keys that belong to the key chain, and specify how long each key is valid. Each key has its own key identifier (specified with the key number key chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use.

You can configure multiple keys with life times. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters. The lifetimes allow for overlap during key changes. Note that the router must know these lifetimes.
Beginning in privileged EXEC mode, follow these steps to manage authentication keys:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>key chain name-of-chain</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>key number</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>key-string text</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>accept-lifetime start-time {infinite</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>send-lifetime start-time {infinite</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show key chain</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the key chain, use the **no key chain name-of-chain** global configuration command.
Monitoring and Maintaining the IP Network

You can remove all contents of a particular cache, table, or database. You can also display specific statistics. Use the privileged EXEC commands in Table 37-17 to clear routes or display status:

**Table 37-17  Commands to Clear IP Routes or Display Route Status**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip route {network [mask l *]}</td>
<td>Clear one or more routes from the IP routing table.</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Display the parameters and state of the active routing protocol process.</td>
</tr>
<tr>
<td>show ip route [address [mask] [longer-prefixes]</td>
<td>Display the current state of the routing table.</td>
</tr>
<tr>
<td>[protocol [process-id]]</td>
<td>Display the current state of the routing table in summary form.</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>Display supernets.</td>
</tr>
<tr>
<td>show ip route supernets-only</td>
<td>Display the routing table used to switch IP traffic.</td>
</tr>
<tr>
<td>show ip cache</td>
<td>Display all route maps configured or only the one specified.</td>
</tr>
<tr>
<td>show route-map [map-name]</td>
<td></td>
</tr>
</tbody>
</table>
This chapter describes how to configure IPv6 unicast routing on the Catalyst 3560 switch.

**Note**

To use all IPv6 features in this chapter, switch the stack must be running the IP services image. Switches running the IP base image support only IPv6 static routing and RIP for IPv6.

For information about configuring IPv6 Multicast Listener Discovery (MLD) snooping, see Chapter 39, “Configuring IPv6 MLD Snooping.” For information on configuring IPv6 access control lists (ACLs), see Chapter 40, “Configuring IPv6 ACLs.” For information about configuring IPv4 unicast routing, see Chapter 37, “Configuring IP Unicast Routing.”

To enable IPv6 routing, you must configure the switch to use a dual IPv4 and IPv6 switch database management (SDM) template. See the “Dual IPv4 and IPv6 Protocol Stacks” section on page 38-5.

**Note**

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS documentation referenced in the procedures.

This chapter consists of these sections:

- “Understanding IPv6” section on page 38-2
- “Configuring IPv6” section on page 38-10
- “Displaying IPv6” section on page 38-26
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
- Use the Search field to locate the Cisco IOS software documentation. For example, if you want information about static routes, you can enter Implementing Static Routes for IPv6 in the search field to get this document about static routes: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes_ps6441_TSD_Products_Configuration_Guide_Chapter.html

This section describes IPv6 implementation on the switch.
- IPv6 Addresses, page 38-2
- Supported IPv6 Unicast Routing Features, page 38-3
- Unsupported IPv6 Unicast Routing Features, page 38-8
- Limitations, page 38-9

IPv6 Addresses

The switch supports only IPv6 unicast addresses. It does not support site-local unicast addresses, anycast addresses, or multicast 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::09C0:080F:130B

For more information about IPv6 address formats, address types, and the IPv6 packet header, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of Cisco IOS IPv6 Configuration Library on Cisco.com.

In the “Implementing Addressing and Basic Connectivity” chapter, these sections apply to the Catalyst 3560 switch:
- IPv6 Address Formats
- IPv6 Address Type: Unicast
Supported IPv6 Unicast Routing Features

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

- 128-Bit Wide Unicast Addresses, page 38-3
- DNS for IPv6, page 38-4
- Path MTU Discovery for IPv6 Unicast, page 38-4
- ICMPv6, page 38-4
- Neighbor Discovery, page 38-4
- Default Router Preference, page 38-5
- IPv6 Stateless Autoconfiguration and Duplicate Address Detection, page 38-5
- IPv6 Applications, page 38-5
- Dual IPv4 and IPv6 Protocol Stacks, page 38-5
- DHCP for IPv6 Address Assignment, page 38-6
- Static Routes for IPv6, page 38-6
- RIP for IPv6, page 38-7
- OSPF for IPv6, page 38-7 (only on switches running the IP services image)
- EIGRP for IPv6, page 38-7 (only on switches running the IP services image)
- HSRP for IPv6, page 38-7 (only on switches running the IP services image)
- SNMP and Syslog Over IPv6, page 38-7
- HTTP(S) Over IPv6, page 38-8

Support on the switch includes expanded address capability, header format simplification, improved support of extensions and options, and hardware parsing of the extension header. The switch supports hop-by-hop extension header packets, which are routed or bridged in software.

The switch provides IPv6 routing capability over native Ethernet Inter-Switch Link (ISL) or 802.1Q trunk ports for static routes, Routing Information Protocol (RIP) for IPv6, and Open Shortest Path First (OSPF) Version 3 Protocol. It supports up to 16 equal-cost routes and can simultaneously forward IPv4 and IPv6 frames at line rate.

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.

**DNS for IPv6**

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.

**Path MTU Discovery for IPv6 Unicast**

The switch supports advertising the system maximum transmission unit (MTU) to IPv6 nodes and path MTU discovery. Path MTU discovery allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path. In IPv6, if a link along the path is not large enough to accommodate the packet size, the source of the packet handles the fragmentation. The switch does not support path MTU discovery for multicast packets.

**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.
Default Router Preference

The switch supports IPv6 default router preference (DRP), an extension in router advertisement messages. DRP improves the ability of a host to select an appropriate router, especially when the host is multihomed and the routers are on different links. The switch does not support the Route Information Option in RFC 4191.

An IPv6 host maintains a default router list from which it selects a router for traffic to offlink destinations. The selected router for a destination is then cached in the destination cache. NDP for IPv6 specifies that routers that are reachable or probably reachable are preferred over routers whose reachability is unknown or suspect. For reachable or probably reachable routers, NDP can either select the same router every time or cycle through the router list. By using DRP, you can configure an IPv6 host to prefer one router over another, provided both are reachable or probably reachable.

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

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, Telnet, TFTP, and FTP
- 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 “Managing Cisco IOS Applications over IPv6” chapter and the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.

Dual IPv4 and IPv6 Protocol Stacks

You must use the dual IPv4 and IPv6 template to allocate ternary content addressable memory (TCAM) usage to both IPv4 and IPv6 protocols.

Figure 38-1 shows a router forwarding both IPv4 and IPv6 traffic through the same interface, based on the IP packet and destination addresses.
Understanding IPv6

Use the dual IPv4 and IPv6 switch database management (SDM) template to enable IPv6 routing. For more information about the dual IPv4 and IPv6 SDM template, see Chapter 7, “Configuring SDM Templates.”

The dual IPv4 and IPv6 templates allow the switch to be used in dual stack environments.

- If you try to configure IPv6 without first selecting a dual IPv4 and IPv6 template, a warning message appears.
- In IPv4-only environments, the switch routes IPv4 packets and applies IPv4 QoS and ACLs in hardware. IPv6 packets are not supported.
- In dual IPv4 and IPv6 environments, the switch routes both IPv4 and IPv6 packets and applies IPv4 QoS in hardware.
- Full IPv6 QoS is not supported. IPv6 QoS trust is supported.
- If you do not plan to use IPv6, do not use the dual stack template because this template results in less TCAM capacity for each resource.

For more information about IPv4 and IPv6 protocol stacks, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter of Cisco IOS IPv6 Configuration Library on Cisco.com.

DHCP for IPv6 Address Assignment

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The address assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface, on multiple interfaces, or the server can automatically find the appropriate pool.

This document describes only the DHCPv6 address assignment. For more information about configuring the DHCPv6 client, server, or relay agent functions, see the “Implementing DHCP for IPv6” chapter in 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.
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 more information about RIP for IPv6, see the “Implementing RIP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

### OSPF for IPv6

The switch running the IP services image supports Open Shortest Path First (OSPF) for IPv6, a link-state protocol for IP. For more information, see the “Implementing OSFP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

### EIGRP for IPv6

The switch running the IP services image supports Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6. It is configured on the interfaces on which it runs and does not require a global IPv6 address.

Before running, an instance of EIGRP IPv6 requires an implicit or explicit router ID. An implicit router ID is derived from a local IPv4 address, so any IPv4 node always has an available router ID. However, EIGRP IPv6 might be running in a network with only IPv6 nodes and therefore might not have an available IPv4 router ID.

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

### HSRP for IPv6

The switch running the IP services image supports the Hot Standby Router Protocol (HSRP) for IPv6. HSRP provides routing redundancy for routing IPv6 traffic not dependent on the availability of any single router. IPv6 hosts learn of available routers through IPv6 neighbor discovery router advertisement messages. These messages are multicast periodically or are solicited by hosts.

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. Periodic messages are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These messages stop after a final one is sent when the group leaves the active state.

For more information about configuring HSRP for IPv6, see the “Configuring First Hop Redundancy Protocols in 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.
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.

**Unsupported IPv6 Unicast Routing Features**

The switch does not support these IPv6 features:

- IPv6 policy-based routing
- IPv6 virtual private network (VPN) routing and forwarding (VRF) table support
- Support for IPv6 routing protocols: multiprotocol Border Gateway Protocol (BGP) and Intermediate System-to-Intermediate System (IS-IS) routing
- IPv6 packets destined to site-local addresses
- Tunneling protocols, such as IPv4-to-IPv6 or IPv6-to-IPv4
• The switch as a tunnel endpoint supporting IPv4-to-IPv6 or IPv6-to-IPv4 tunneling protocols
• IPv6 unicast reverse-path forwarding
• IPv6 general prefixes

**Limitations**

Because IPv6 is implemented in switch hardware, some limitations occur due to the IPv6 compressed addresses in the TCAM. These hardware limitations result in some loss of functionality and limits some features.

These are feature limitations.

- **ICMPv6 redirect functionality is not supported** for IPv6 host routes (routes used to reach a specific host) or for IPv6 routes with masks greater than 64 bits. The switch cannot redirect hosts to a better first-hop router for a specific destination that is reachable through a host route or through a route with masks greater than 64 bits.
- **Load balancing using equal cost and unequal cost routes is not supported** for IPv6 host routes or for IPv6 routes with a mask greater than 64 bits.
- **The switch cannot forward SNAP-encapsulated IPv6 packets.**

| Note | There is a similar limitation for IPv4 SNAP-encapsulated packets, but the packets are dropped at the switch and are not forwarded. |

- **The switch routes IPv6-to-IPv4 and IPv4-to-IPv6 packets in hardware, but the switch cannot be an IPv6-to-IPv4 or IPv4-to-IPv6 tunnel endpoint.**
- **Bridged IPv6 packets with hop-by-hop extension headers are forwarded in software. In IPv4, these packets are routed in software, but bridged in hardware.**
- **Interface counters for IPv6 traffic include software-forwarded traffic only; hardware-switched traffic is excluded.**
- **In addition to the normal SPAN and RSPAN limitations defined in the software configuration guide, these limitations are specific to IPv6 packets:**
  - When you send RSPAN IPv6-routed packets, the source MAC address in the SPAN output packet can be incorrect.
  - When you send RSPAN IPv6-routed packets, the destination MAC address can be incorrect. Normal traffic is not affected.
- **The switch cannot apply QoS classification or policy-based routing on source-routed IPv6 packets in hardware.**
- **The switch cannot generate ICMPv6 Packet Too Big messages for multicast packets.**
Configuring IPv6

These sections contain this IPv6 forwarding configuration information:
- Default IPv6 Configuration, page 38-10
- Configuring IPv6 Addressing and Enabling IPv6 Routing, page 38-11
- Configuring Default Router Preference, page 38-13
- Configuring IPv4 and IPv6 Protocol Stacks, page 38-13
- Configuring DHCP for IPv6 Address Assignment, page 38-15
- Configuring IPv6 ICMP Rate Limiting, page 38-18
- Configuring CEF for IPv6, page 38-18
- Configuring Static Routes for IPv6, page 38-19
- Configuring RIP for IPv6, page 38-20
- Configuring OSPF for IPv6, page 38-21
- Configuring EIGRP for IPv6, page 38-23
- Configuring HSRP for IPv6, page 38-23

Default IPv6 Configuration

Table 38-1 shows the default IPv6 configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDM template</td>
<td>Default</td>
</tr>
<tr>
<td>IPv6 routing</td>
<td>Disabled globally and on all interfaces.</td>
</tr>
<tr>
<td>CEFv6 or dCEFv6</td>
<td>Disabled (IPv4 CEF and dCEF are enabled by default).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When IPv6 routing is enabled, CEFv6 and dCEFv6 are automatically enabled.</td>
</tr>
<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 these guidelines:

- Be sure to select a dual IPv4 and IPv6 SDM template.
- Not all features discussed in this chapter are supported by the Catalyst 3560 switch running the IP services image. See the “Unsupported IPv6 Unicast Routing Features” section on page 38-8.
- 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 FF02:0:0:0:0:1:ff00::/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 routing:

<table>
<thead>
<tr>
<th>Command</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> sdm prefer dual-ipv4-and-ipv6 {default</td>
<td>routing</td>
</tr>
<tr>
<td></td>
<td>- <strong>default</strong>—Set the switch to the default template to balance system resources.</td>
</tr>
<tr>
<td></td>
<td>- <strong>routing</strong>—Set the switch to the routing template to support IPv4 and IPv6 routing, including IPv4 policy-based routing.</td>
</tr>
<tr>
<td></td>
<td>- <strong>vlan</strong>—Maximize VLAN configuration on the switch with no routing supported in hardware.</td>
</tr>
<tr>
<td><strong>Step 3</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> reload</td>
<td>Reload the operating system.</td>
</tr>
<tr>
<td><strong>Step 5</strong> configure terminal</td>
<td>Enter global configuration mode after the switch reloads.</td>
</tr>
<tr>
<td><strong>Step 6</strong> interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure. The interface can be a physical interface, a switch virtual interface (SVI), or a Layer 3 EtherChannel.</td>
</tr>
<tr>
<td><strong>Step 7</strong> no switchport</td>
<td>Remove the interface from Layer 2 configuration mode (if it is a physical interface).</td>
</tr>
</tbody>
</table>
To remove an IPv6 address from an interface, use the **no ipv6 address ipv6-prefix/prefix length eui-64** or **no ipv6 address ipv6-address link-local** interface configuration command. To remove all manually configured IPv6 addresses from an interface, use the **no ipv6 address** interface configuration command without arguments. To disable IPv6 processing on an interface that has not been explicitly configured with an IPv6 address, use the **no ipv6 enable** interface configuration command. To globally disable IPv6 routing, use the **no ipv6 unicast-routing** global configuration command.

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 shows how the interface ID (20B:46FF:FE2F:D940) is appended to the link-local prefix FE80::/64 of the interface.

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch(config)# show ipv6 interface gigabitethernet0/1
GigabitEthernet0/1 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
```
Configuring Default Router Preference

Router advertisement messages are sent with the default router preference (DRP) configured by the `ipv6 nd router-preference` interface configuration command. If no DRP is configured, RAs are sent with a medium preference.

A DRP is useful when two routers on a link might provide equivalent, but not equal-cost routing, and policy might dictate that hosts should prefer one of the routers.

Beginning in privileged EXEC mode, follow these steps to configure a DRP for a router on an interface.

Step 1
configure terminal

Step 2
interface interface-id

Step 3
ipv6 nd router-preference { high | medium | low }

Step 4
end

Step 5
show ipv6 interface

Step 6
copy running-config startup-config

Use the `no ipv6 nd router-preference` interface configuration command to disable an IPv6 DRP.

This example shows how to configure a DRP of `high` for the router on an interface.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config)# ipv6 nd router-preference high
Switch(config-if)# end
```

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

Configuring IPv4 and IPv6 Protocol Stacks

Before configuring IPv6 routing, you must select an SDM template that supports IPv4 and IPv6. If not already configured, use the `sdm prefer dual-ipv4-and-ipv6 { default | routing | vlan } [ desktop ]` global configuration command to configure a template that supports IPv6. When you select a new template, you must reload the switch by using the `reload` privileged EXEC command so that the template takes effect.
Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 interface to support both IPv4 and IPv6 and to enable IPv6 routing.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip routing</td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 unicast-routing</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>no switchport</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip address ip-address mask [secondary]</td>
</tr>
<tr>
<td>Step 7</td>
<td>ipv6 address ipv6-prefix/prefix length eui-64</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td>Step 9</td>
<td>show interface interface-id</td>
</tr>
<tr>
<td></td>
<td>show ip interface interface-id</td>
</tr>
<tr>
<td></td>
<td>show ipv6 interface interface-id</td>
</tr>
<tr>
<td>Step 10</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable IPv4 routing, use the no ip routing global configuration command. To disable IPv6 routing, use the no ipv6 unicast-routing global configuration command. To remove an IPv4 address from an interface, use the no ip address ip-address mask interface configuration command. To remove an IPv6 address from an interface, use the no ipv6 address ipv6-prefix/prefix length eui-64 or no ipv6 address ipv6-address link-local interface configuration command. To remove all manually configured IPv6 addresses from an interface, use the no ipv6 address interface configuration command without arguments. To disable IPv6 processing on an interface that has not been explicitly configured with an IPv6 address, use the no ipv6 enable interface configuration command.

This example shows how to enable IPv4 and IPv6 routing on an interface.

Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 244.244.244.0
Switch(config-if)# ipv6 address 2001:0DB8::c18:1::/64 eui 64
Switch(config-if)# end
Chapter 38  Configuring IPv6 Unicast Routing

Configuring DHCP for IPv6 Address Assignment

These sections describe how to configure Dynamic Host Configuration Protocol for IPv6 (DHCPv6) address assignment:

- Default DHCPv6 Address Assignment Configuration, page 38-15
- DHCPv6 Address Assignment Configuration Guidelines, page 38-15
- Enabling DHCPv6 Server Function, page 38-15
- Enabling DHCPv6 Client Function, page 38-17

Default DHCPv6 Address Assignment Configuration

By default, no DHCPv6 features are configured on the switch.

DHCPv6 Address Assignment Configuration Guidelines

When configuring DHCPv6 address assignment, consider these guidelines:

- In the procedures, the specified interface must be one of these Layer 3 interfaces:
  - DHCPv6 IPv6 routing must be enabled on a Layer 3 interface.
  - SVI: a VLAN interface created by using the `interface vlan vlan_id` command.
  - EtherChannel port channel in Layer 3 mode: a port-channel logical interface created by using the `interface port-channel port-channel-number` command.
- Before configuring DHCPv6, you must select a Switch Database Management (SDM) template that supports IPv4 and IPv6.
- The switch can act as a DHCPv6 client, server, or relay agent. The DHCPv6 client, server, and relay function are mutually exclusive on an interface.

Enabling DHCPv6 Server Function

Beginning in privileged EXEC mode, follow these steps to enable the DHCPv6 server function on an interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ipv6 dhcp pool poolname</code> Enter DHCP pool configuration mode, and define the name for the IPv6 DHCP pool. The pool name can be a symbolic string (such as Engineering) or an integer (such as 0).</td>
</tr>
<tr>
<td>Step 3</td>
<td>`address prefix IPv6-prefix lifetime [t1 t1</td>
</tr>
</tbody>
</table>
To delete a DHCPv6 pool, use the no ipv6 dhcp pool poolname global configuration command. Use the no form of the DHCP pool configuration mode commands to change the DHCPv6 pool characteristics.

To disable the DHCPv6 server function on an interface, use the no ipv6 dhcp server interface configuration command.
This example shows how to configure a pool called *engineering* with an IPv6 address prefix:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)# address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

This example shows how to configure a pool called *testgroup* with three link-addresses and an IPv6 address prefix:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool testgroup
Switch(config-dhcpv6)# link-address 2001:1001::0/64
Switch(config-dhcpv6)# link-address 2001:1002::0/64
Switch(config-dhcpv6)# link-address 2001:2000::0/48
Switch(config-dhcpv6)# address prefix 2001:1003::0/64
Switch(config-dhcpv6)# end
```

This example shows how to configure a pool called *350* with vendor-specific options:

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

### Enabling DHCPv6 Client Function

Beginning in privileged EXEC mode, follow these steps to enable DHCPv6 client function on an interface.

<table>
<thead>
<tr>
<th>Command</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> interface interface-id</td>
<td>Enter interface configuration mode, and specify the interface to configure.</td>
</tr>
<tr>
<td><strong>Step 3</strong> ipv6 address dhcp [rapid-commit]</td>
<td>Enable the interface to acquire an IPv6 address from the DHCPv6 server.</td>
</tr>
<tr>
<td></td>
<td><strong>rapid-commit</strong>—(Optional) Allow two-message exchange method for address assignment.</td>
</tr>
<tr>
<td><strong>Step 4</strong> ipv6 dhcp client request [vendor-specific]</td>
<td>(Optional) Enable the interface to request the vendor-specific option.</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show ipv6 dhcp interface</td>
<td>Verify that the DHCPv6 client is enabled on an interface.</td>
</tr>
</tbody>
</table>

To disable the DHCPv6 client function, use the `no ipv6 address dhcp` interface configuration command. To remove the DHCPv6 client request, use the `no ipv6 address dhcp client request` interface configuration command.

This example shows how to acquire an IPv6 address and to enable the rapid-commit option:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```
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.

Beginning in privileged EXEC mode, follow these steps to change the ICMP rate-limiting parameters:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 icmp error-interval interval [bucketsize]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ipv6 interface [interface-id]</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To return to the default configuration, use the no ipv6 icmp error-interval global configuration command.

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 CEF for IPv6

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology to improve network performance. IPv6 CEF is disabled by default but are automatically enabled when you configure IPv6 routing.

To route IPv6 unicast packets, you must first globally configure IPv6 unicast packet forwarding by using the ipv6 unicast-routing global configuration command. You must configure an IPv6 address and IPv6 processing on an interface by using the ipv6 address interface configuration command.

To disable IPv6 CEF, use the no ipv6 cef global configuration command. To reenable IPv6 CEF or dCEF if it has been disabled, use the ipv6 cef global configuration command. You can verify the IPv6 state by entering the show ipv6 cef privileged EXEC command.

For more information about configuring CEF and dCEF, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the Cisco IOS IPv6 Configuration Library on Cisco.com.
### Configuring Static Routes for IPv6

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.

Beginning in privileged EXEC mode, follow these steps to configure an IPv6 static route:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>`ipv6 route ipv6-prefix/prefix length [ipv6-address</td>
<td>interface-id [ipv6-address]] [administrative distance]`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>ipv6-prefix</code>—The IPv6 network that is the destination of the static route. It can also be a hostname when static host routes are configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>/prefix length</code>—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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>ipv6-address</code>—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 specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>interface-id</code>—Specify 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> You must specify an <code>interface-id</code> 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></td>
<td>- <code>administrative distance</code>—(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>
<tr>
<td>3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Chapter 38 Configuring IPv6 Unicast Routing

Configuring IPv6

To remove a configured static route, use the `no ipv6 route ipv6-prefix/prefix length {ipv6-address | interface interface-id} [administrative distance]` global configuration command.

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

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet0/1 130
```

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.

Configuring RIP for IPv6

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.

Beginning in privileged EXEC mode, follow these required and optional steps to configure IPv6 RIP:

```
Command | Purpose
---- | ----
Step 1 configure terminal | Enter global configuration mode.
Step 2 ipv6 router rip name | Configure an IPv6 RIP routing process, and enter router configuration mode for the process.
Step 3 maximum-paths number-paths | (Optional) Define the maximum number of equal-cost routes that IPv6 RIP can support. The range is from 1 to 64, and the default is 4 routes.
Step 4 exit | Return to global configuration mode.
Step 5 interface interface-id | Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 6 ipv6 rip name enable | Enable the specified IPv6 RIP routing process on the interface.
```
To disable a RIP routing process, use the `no ipv6 router rip name` command. To disable the RIP routing process for an interface, use the `no ipv6 rip name` command.

This example shows how to enable the RIP routing process with a maximum of eight equal-cost routes and to enable it on an interface:

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config-router)# exit
Switch(config-if)# ipv6 rip cisco enable
```

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

## Configuring OSPF for IPv6

You can customize OSPF for IPv6 for your network. However, the defaults for OSPF in IPv6 are set to meet the requirements of most customers and features.

Follow these guidelines:

- The switch must be running the IP services image.
- Be careful when changing the defaults for IPv6 commands. Changing the defaults might adversely affect OSPF for the IPv6 network.
- Before you enable IPv6 OSPF on an interface, 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 Layer 3 interfaces on which you are enabling IPv6 OSPF.
Beginning in privileged EXEC mode, follow these required and optional steps to configure IPv6 OSPF:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1   configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2   ipv6 router ospf process-id</td>
<td>Enable OSPF router configuration mode for the process. The process ID is the number administratively assigned when enabling the OSPF for IPv6 routing process. It is locally assigned and can be a positive integer from 1 to 65535.</td>
</tr>
</tbody>
</table>
| Step 3   area area-id range {ipv6-prefix/prefix length} [advertise | (Optional) Consolidate and summarize routes at an area boundary.  
|         | not-advertise] [cost cost]                                              |
|         | • area-id—Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IPv6 prefix.  
|         | • ipv6-prefix/prefix length—The destination IPv6 network and 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.  
|         | • advertise—(Optional) Set the address range status to advertise and to generate a Type 3 summary link-state advertisement (LSA).  
|         | • not-advertise—(Optional) Set the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and component networks remain hidden from other networks.  
|         | • cost cost—(Optional) Metric or cost for this summary route, which is used during OSPF SPF calculation to determine the shortest paths to the destination. The value can be 0 to 16777215. |
| Step 4   maximum paths number-paths | (Optional) Define the maximum number of equal-cost routes to the same destination that IPv6 OSPF should enter in the routing table. The range is from 1 to 64, and the default is 16. |
| Step 5   exit                      | Return to global configuration mode.                                   |
| Step 6   interface interface-id   | Enter interface configuration mode, and specify the Layer 3 interface to configure. |
| Step 7   ipv6 ospf process-id area area-id [instance instance-id] | Enable OSPF for IPv6 on the interface.  
|         | instance instance-id—(Optional) Instance identifier.                  |
| Step 8   end                       | Return to privileged EXEC mode.                                        |
| Step 9   show ipv6 ospf [process-id] [area-id] interface [interface-id] | Display information about OSPF interfaces.  
|         | or show ipv6 ospf [process-id] [area-id]                               | Display general information about OSPF routing processes.  
| Step 10  copy running-config startup-config | (Optional) Save your entries in the configuration file.                 |
To disable an OSPF routing process, use the no **ipv6 router ospf** process-id global configuration command. To disable the OSPF routing process for an interface, use the no **ipv6 ospf process-id area area-id** interface configuration command.

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

### Configuring EIGRP for IPv6

By default, EIGRP for IPv6 is disabled. You can configure EIGRP for IPv6 on an interface. After configuring the router and the interface for EIGRP, enter the **no shutdown** privileged EXEC command to start EIGRP.

**Note**

If EIGRP for IPv6 is not in shutdown mode, EIGRP might start running before you enter the EIGRP router-mode commands to configure the router and the interface.

The switch must be running the IP services image.

To set an explicit router ID, use the **show ipv6 eigrp** command to see the configured router IDs, and then use the **router-id** command.

As with EIGRP IPv4, you can use EIGRPv6 to specify your EIGRP IPv4 interfaces and to select a subset of those as passive interfaces. Use the **passive-interface default** command to make all interfaces passive, and then use the **no passive-interface** command on selected interfaces to make them active. EIGRP IPv6 does not need to be configured on a passive interface.

For more configuration procedures, see the “Implementing EIGRP for IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

### Configuring HSRP for IPv6

Hot Standby Router Protocol (HSRP) for IPv6 provides routing redundancy for routing IPv6 traffic not dependent on the availability of any single router.

When HSRP for IPv6 is enabled on a switch, IPv6 hosts learn of available IPv6 routers through IPv6 neighbor discovery router advertisement messages. An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number. The group has a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. Periodic messages are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active.

The switch must be running the IP services image.

When configuring HSRP for IPv6, you must enable HSRP version 2 (HSRPv2) on the interface.

For configuration guidelines when configuring HSRP for IPv6 with HSRPv1 and HSRPv2, see the “HSRP Configuration Guidelines” section on page 41-6 and the “Troubleshooting HSRP” section on page 41-13.

For more information about HSRP for IPv6 and HSRPv2, see the Chapter 41, “Configuring HSRP.”

**Note**

Before configuring an HSRP for IPv6 group, you must enable the forwarding of IPv6 packets by using the **ipv6 unicast-routing** global configuration command and enable IPv6 on the interface on which you will configure an HSRP for IPv6 group.
### Enabling HSRP Version 2

Beginning in privileged EXEC mode, follow these steps to enable HSRP version 2 on a Layer 3 interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the Layer 3 interface on which you want to specify the standby version.</td>
</tr>
<tr>
<td>Step 3 standby version {1</td>
<td>2}</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show standby</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### Enabling an HSRP Group for IPv6

Beginning in privileged EXEC mode, follow these steps to create or enable HSRP for IPv6 on a Layer 3 interface.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Enter interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP for IPv6.</td>
</tr>
<tr>
<td>Step 3 standby [group-number] ipv6 {link-local-address</td>
<td>autoconfig]</td>
</tr>
<tr>
<td></td>
<td>• (Optional) group-number—The group number on the interface for which HSRP is being enabled. The range is 0 to 4095. The default is 0. If there is only one HSRP group, you do not need to enter a group number.</td>
</tr>
<tr>
<td></td>
<td>• Enter the link-local address of the Hot Standby router interface, or enable the link-local address to be generated automatically from the link-local prefix and a modified EUI-64 format interface identifier, where the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.</td>
</tr>
</tbody>
</table>
Use the `no standby [group-number] ipv6` interface configuration command to disable HSRP for IPv6.

This example shows how to activate HSRP for IPv6 for group 1 on a port. The IP address used by the hot standby group is learned by using HSRP for IPv6.

**Note**

This procedure is the minimum number of steps required to enable HSRP for IPv6. Other configurations are optional.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ipv6 autoconfig
Switch(config-if)# end
Switch# show standby
```

For more information about configuring HSRP for IPv6, see the “Configuring First Hop Redundancy Protocols in IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.
Displaying IPv6

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

Table 38-2 shows the privileged EXEC commands for monitoring IPv6 on the switch.

Table 38-2 Commands for Monitoring IPv6

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

Table 38-3 shows the privileged EXEC command for displaying EIGRP IPv6 information.

Table 38-3 Commands for Displaying EIGRP IPv6 Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 eigrp [as-number] interface</td>
<td>Displays information about interfaces configured for EIGRP IPv6.</td>
</tr>
<tr>
<td>show ipv6 eigrp [as-number] neighbor</td>
<td>Displays the neighbors discovered by EIGRP IPv6.</td>
</tr>
<tr>
<td>show ipv6 eigrp [as-number] traffic</td>
<td>Displays the number of EIGRP IPv6 packets sent and received.</td>
</tr>
<tr>
<td>show ipv6 eigrp topology [as-number</td>
<td>ipv6-address] [active</td>
</tr>
</tbody>
</table>
Table 38-4 shows the privileged EXEC commands for displaying information about IPv4 and IPv6 address types.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip http server history</td>
<td>Display the previous 20 connections to the HTTP server, including the IP address accessed and the time when the connection was closed.</td>
</tr>
<tr>
<td>show ip http server connection</td>
<td>Display the current connections to the HTTP server, including the local and remote IP addresses being accessed.</td>
</tr>
<tr>
<td>show ip http client connection</td>
<td>Display the configuration values for HTTP client connections to HTTP servers.</td>
</tr>
<tr>
<td>show ip http client history</td>
<td>Display a list of the last 20 requests made by the HTTP client to the server.</td>
</tr>
</tbody>
</table>

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>
```

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

```
Switch# show ipv6 cef
::/0
  nexthop 3FFE:C000:0:7::777 Vlan7
  3FFE:C000:0:1::/64
    attached to Vlan1
  3FFE:C000:0:1:20B:46FF:FE2F:D940/128
    receive
  3FFE:C000:0:7::/64
    attached to Vlan7
  3FFE:C000:0:7::777/128
    attached to Vlan7
  3FFE:C000:0:7:20B:46FF:FE2F:D97F/128
    receive
  3FFE:C000:111:1::/64
    attached to FastEthernet1/0/11
  3FFE:C000:111:1:20B:46FF:FE2F:D945/128
    receive
  3FFE:C000:168:1::/64
    attached to FastEthernet2/0/43
  3FFE:C000:168:1:20B:46FF:FE2F:D94B/128
    receive
```
Displaying IPv6

3FFE:C000:16A:1::/64
attached to Loopback10

3FFE:C000:16A:1:20B:46FF:FE2F:D900/128
receive

<output truncated>

This is an example of the output from the **show ipv6 protocols** privileged EXEC command:

Switch# **show ipv6 protocols**
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "rip fer"
**Interfaces:**
Vlan6
FastEthernet0/4
FastEthernet0/11
FastEthernet0/12
**Redistribution:**
None

This is an example of the output from the **show ipv6 rip** privileged EXEC command:

Switch# **show ipv6 rip**
RIP process "fer", port 521, multicast-group FF02::9, pid 190
Administrative distance is 120. Maximum paths is 16
Updates every 30 seconds, expire after 180
Holddown lasts 0 seconds, garbage collect after 120
Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 9040, trigger updates 60
**Interfaces:**
Vlan6
FastEthernet2/0/4
FastEthernet2/0/11
FastEthernet1/0/12
**Redistribution:**
None

This is an example of the output from the **show ipv6 static** privileged EXEC command:

Switch# **show ipv6 static**
IPv6 Static routes
Code: * - installed in RIB
* ::/0 via nexthop 3FFE:C000:0:7::777, distance 1

This is an example of the output from the **show ipv6 neighbor** privileged EXEC command:

Switch# **show ipv6 neighbors**
IPv6 Address Age Link-layer Addr State Interface
3FFE:C000:0:7::777 - 0007.0007.0007 REACH V17
3FFE:C101:113:1::33 - 0000.0000.0033 REACH Fa1/0/13

This is an example of the output from the **show ipv6 route** privileged EXEC command:

Switch# **show ipv6 route**
IPv6 Routing Table - Default - 1 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
L FF00::/8 [0/0]
via Null0, receive
This is an example of the output from the `show ipv6 traffic` privileged EXEC command.

```
Switch# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
    0 source-routed, 0 truncated
    0 format errors, 0 hop count exceeded
    0 bad header, 0 unknown option, 0 bad source
    0 unknown protocol, 0 not a router
    0 fragments, 0 total reassembled
    0 reassembly timeouts, 0 reassembly failures
  Sent:  36861 generated, 0 forwarded
    0 fragmented into 0 fragments, 0 failed
    0 encapsulation failed, 0 no route, 0 too big
    0 RPF drops, 0 RPF suppressed drops
Mcast: 1 received, 36861 sent

ICMP statistics:
  Rcvd:  1 input, 0 checksum errors, 0 too short
    0 unknown info type, 0 unknown error type
    unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
    parameter: 0 error, 0 header, 0 option
    0 hopcount expired, 0 reassembly timeout,0 too big
    0 echo request, 0 echo reply
    0 group query, 0 group report, 0 group reduce
    1 router solicit, 0 router advert, 0 redirects
    0 neighbor solicit, 0 neighbor advert
  Sent: 10112 output, 0 rate-limited
    unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
    parameter: 0 error, 0 header, 0 option
    0 hopcount expired, 0 reassembly timeout,0 too big
    0 echo request, 0 echo reply
    0 group query, 0 group report, 0 group reduce
    0 router solicit, 9944 router advert, 0 redirects
    0 neighbor solicit, 84 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
    0 no port, 0 dropped
  Sent: 26749 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```
CHAPTER 40

Configuring IPv6 ACLs

This chapter includes information about configuring IPv6 ACLs on the Catalyst 3560 switch. 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. You can also create and apply input router ACLs to filter Layer 3 management traffic.

Note

To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. You select the template by entering the `sdm prefer {default | dual-ipv4-and-ipv6}` global configuration command.

For related information, see these chapters:
- For more information about SDM templates, see Chapter 7, “Configuring SDM Templates.”
- For information about ACLs on the switch, see Chapter 40, “Configuring IPv6 ACLs.”

Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

This chapter contains these sections:
- Understanding IPv6 ACLs, page 40-1
- Configuring IPv6 ACLs, page 40-3
- Displaying IPv6 ACLs, page 40-8

Understanding IPv6 ACLs

A switch image supports two types of IPv6 ACLs:

- IPv6 router ACLs
  - Supported on outbound or inbound traffic on Layer 3 interfaces, which can be routed ports, switch virtual interfaces (SVIs), or Layer 3 EtherChannels.
  - Applied to only IPv6 packets that are routed.
Understanding IPv6 ACLs

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

A switch running the IP base image supports only input router IPv6 ACLs. It does not support port ACLs or output IPv6 router ACLs.

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.

For more information about ACL support on the switch, see Chapter 33, “Configuring Network Security with ACLs.”

You can apply both IPv4 and IPv6 ACLs to an interface.

As with IPv4 ACLs, IPv6 port ACLs take precedence over router ACLs:

- When an input router ACL and input port ACL exist in an SVI, packets received on ports to which a port ACL is applied are filtered by the port ACL. Routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.

- When an output router ACL and input port ACL exist in an SVI, packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IPv6 packets are filtered by the router ACL. Other packets are not filtered.

If any port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

These sections describe some characteristics of IPv6 ACLs on the switch:

- Supported ACL Features, page 40-2
- IPv6 ACL Limitations, page 40-3

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.
- Routed or bridged packets with hop-by-hop options have IPv6 ACLs applied in software.
- Logging is supported for router ACLs, but not for port ACLs.
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 and router ACLs for IPv6; it does not support VLAN ACLs (VLAN maps).
- The switch does not apply MAC-based ACLs on IPv6 frames.
- You cannot apply IPv6 port ACLs to Layer 2 EtherChannels.
- The switch does not support output port ACLs.
- Output router ACLs and input port ACLs for IPv6 are supported only on switches. Switches support only control plane (incoming) IPv6 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 or SVIs), the switch checks to determine whether or not the ACL can be supported on the interface. If not, attaching the ACL is rejected.
- If an ACL is applied to an interface and you attempt to add an access control entry (ACE) with an unsupported keyword, the switch does not allow the ACE to be added to the ACL that is currently attached to the interface.

Configuring IPv6 ACLs

Before configuring IPv6 ACLs, you must select one of the dual IPv4 and IPv6 SDM templates.

To filter IPv6 traffic, you perform these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create an IPv6 ACL, and enter IPv6 access list configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure the IPv6 ACL to block (deny) or pass (permit) traffic.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Apply the IPv6 ACL to an interface. For router ACLs, you must also configure an IPv6 address on the Layer 3 interface to which the ACL is applied.</td>
</tr>
</tbody>
</table>
These sections describe how to configure and apply IPv6 ACLs:

- Default IPv6 ACL Configuration, page 40-4
- Interaction with Other Features, page 40-4
- Creating IPv6 ACLs, page 40-4
- Applying an IPv6 ACL to an Interface, page 40-7

**Default IPv6 ACL Configuration**

There are no IPv6 ACLs configured or applied.

**Interaction with Other Features**

Configuring IPv6 ACLs has these interactions with other features or switch characteristics:

- If an IPv6 router ACL is configured to deny a packet, the packet is dropped. A copy of the packet is sent to the Internet Control Message Protocol (ICMP) queue to generate an ICMP unreachable message for the frame.
- If a bridged frame is to be dropped due to a port ACL, the frame is not bridged.
- You can create both IPv4 and IPv6 ACLs on a switch, and you can apply both IPv4 and IPv6 ACLs to the same interface. Each ACL must have a unique name; an error message appears if you try to use a name that is already configured.

  You use different commands to create IPv4 and IPv6 ACLs and to attach IPv4 or IPv6 ACLs to the same Layer 2 or Layer 3 interface. If you use the wrong command to attach an ACL (for example, an IPv4 command to attach an IPv6 ACL), you receive an error message.

- You cannot use MAC ACLs to filter IPv6 frames. MAC ACLs can only filter non-IP frames.
- If the TCAM is full, for any additional configured ACLs, packets are forwarded to the CPU, and the ACLs are applied in software.

**Creating IPv6 ACLs**

Beginning in privileged EXEC mode, follow these steps to create an IPv6 ACL:

<table>
<thead>
<tr>
<th>Command</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>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>ipv6 access-list</code></td>
<td>Define an IPv6 access list name, and enter IPv6 access-list configuration mode.</td>
</tr>
</tbody>
</table>
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. For additional specific parameters for ICMP, TCP, and UDP, see Steps 3b through 3d.

- **The source-ipv6-prefix/prefix-length or destination-ipv6-prefix/prefix-length** is the source or destination IPv6 network or class of networks for which to set deny or permit conditions, specified in hexadecimal and using 16-bit values between colons (see RFC 2373).

- **Enter any** as an abbreviation for the IPv6 prefix ::/0.

- **For host source-ipv6-address or destination-ipv6-address**, enter the source or destination IPv6 host address for which to set deny or permit conditions, specified in hexadecimal using 16-bit values between colons.

- (Optional) **For operator**, specify an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range**. If the operator follows the **source-ipv6-prefix/prefix-length** argument, it must 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 for filtering TCP or UDP, respectively.

- (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 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.

- (Optional) Enter **sequence value** to specify the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.

- (Optional) Enter **time-range name** to specify a time range for the statement.

---

**Command**

<table>
<thead>
<tr>
<th>Step 3a</th>
<th><strong>deny</strong></th>
<th><strong>permit</strong></th>
<th><strong>protocol</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>source-ipv6-prefix/prefix-length</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>any</strong></td>
<td><strong>host</strong></td>
<td><strong>source-ipv6-address</strong></td>
</tr>
<tr>
<td></td>
<td><strong>[operator [port-number]]</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>destination-ipv6-prefix/prefix-length</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>any</strong></td>
<td><strong>host</strong></td>
<td><strong>destination-ipv6-address</strong></td>
</tr>
<tr>
<td></td>
<td><strong>[dscp value]</strong></td>
<td><strong>[fragments]</strong></td>
<td><strong>[log]</strong></td>
</tr>
<tr>
<td></td>
<td><strong>[log-input]</strong></td>
<td><strong>[sequence value]</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>[time-range name]</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Purpose**

Enter **deny** or **permit** to specify whether to deny or permit the packet if conditions are matched. These are the conditions:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3b</td>
<td>deny</td>
<td>(Optional) Define a TCP access list and the access conditions.</td>
</tr>
<tr>
<td></td>
<td>permit</td>
<td>Enter tcp for Transmission Control Protocol. The parameters are the same as those described in Step 3a, with these additional optional parameters:</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>- ack—Acknowledgment bit set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- established—An established connection. A match occurs if the TCP datagram has the ACK or RST bits set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- fin—Finished bit set; no more data from sender.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- neq {port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- psh—Push function bit set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- range {port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- rst—Reset bit set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- syn—Synchronize bit set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- urg—Urgent pointer bit set.</td>
</tr>
<tr>
<td>3c</td>
<td>deny</td>
<td>(Optional) Define a UDP access list and the access conditions.</td>
</tr>
<tr>
<td></td>
<td>permit</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, and the established parameter is not valid for UDP.</td>
</tr>
<tr>
<td>3d</td>
<td>deny</td>
<td>(Optional) Define an ICMP access list and the access conditions.</td>
</tr>
<tr>
<td></td>
<td>permit</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></td>
<td>icmp</td>
<td>- icmp-type—Enter to filter by ICMP message type, a number from 0 to 255.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- icmp-code—Enter to filter ICMP packets that are filtered by the ICMP message code type, a number from 0 to 255.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show ipv6 access-list</td>
<td>Verify the access list configuration.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Use the no deny | permit IPv6 access-list configuration commands with keywords to remove the deny or permit conditions from the specified access list.

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
```

### Applying an IPv6 ACL to an Interface

This section describes how to apply IPv6 ACLs to network interfaces. You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces, or to inbound traffic on Layer 2 interfaces.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>no switchport</td>
</tr>
<tr>
<td>Step 4</td>
<td>ipv6 address ipv6-address</td>
</tr>
<tr>
<td>Step 5</td>
<td>ipv6 traffic-filter access-list-name {in</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no ipv6 traffic-filter access-list-name interface configuration command to remove an access list from an interface.

This example shows how to apply the access list Cisco to outbound traffic on a Layer 3 interface:

```
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```
Displaying 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 in Table 40-1.

Table 40-1  Commands for Displaying IPv6 Access List Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-lists</td>
<td>Display all access lists configured on the switch.</td>
</tr>
<tr>
<td>show ipv6 access-list [access-list-name]</td>
<td>Display all configured IPv6 access list 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-lists` privileged EXEC command. The output shows only IPv6 access lists configured on the switch.

```
Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30

IPv6 access list outbound
  deny udp any any sequence 10
  deny tcp any any eq telnet sequence 20
```
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 Catalyst 3560 switch.

To use IPv6, you must configure the dual IPv4 and IPv6 Switch Database Management (SDM) template on the switch. You select the template by entering the `sdm prefer dual-ipv4-and-ipv6 {default | vlan}` [desktop] global configuration command.

For related information, see these chapters:
- For more information about SDM templates, see Chapter 7, “Configuring SDM Templates.”
- For information about IPv6 on the switch, see Chapter 38, “Configuring IPv6 Unicast Routing.”

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release or the Cisco IOS documentation referenced in the procedures.

This chapter includes these sections:
- “Understanding MLD Snooping” section on page 39-1
- “Configuring IPv6 MLD Snooping” section on page 39-5
- “Displaying MLD Snooping Information” section on page 39-12

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 its directly attached links 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 (MESS), 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 MAC address table is constructed in software and a per-VLAN IPv6 multicast address table is constructed in software and hardware. The switch then performs IPv6 multicast-address based bridging in hardware.

These sections describe some parameters of IPv6 MLD snooping:

- MLD Messages, page 39-2
- MLD Queries, page 39-2
- Multicast Client Aging Robustness, page 39-3
- Multicast Router Discovery, page 39-3
- MLD Reports, page 39-4
- MLD Done Messages and Immediate-Leave, page 39-4
- Topology Change Notification Processing, page 39-4

**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 MAC-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.

**Note**

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 3560 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.

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 and an IPv6 multicast MAC address are 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.

**Configuring IPv6 MLD Snooping**

These sections describe how to configure IPv6 MLD snooping:

- Default MLD Snooping Configuration, page 39-6
- MLD Snooping Configuration Guidelines, page 39-6
- Enabling or Disabling MLD Snooping, page 39-7
- Configuring a Static Multicast Group, page 39-8
- Configuring a Multicast Router Port, page 39-8
- Enabling MLD Immediate Leave, page 39-9
- Configuring MLD Snooping Queries, page 39-10
- Disabling MLD Listener Message Suppression, page 39-11
Default MLD Snooping Configuration

Table 39-1 shows the default MLD snooping configuration.

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

MLD Snooping Configuration Guidelines

When configuring MLD snooping, consider these guidelines:

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

- When the IPv6 multicast router is a Catalyst 6500 switch and you are using extended VLANs (in the range 1006 to 4094), IPv6 MLD snooping must be enabled on the extended VLAN on the Catalyst 6500 switch in order for the Catalyst 3560 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 multicast entries allowed on the switch or is determined by the configured SDM template.

- The maximum number of address entries allowed for the switch is 1000.
Enabling or Disabling MLD Snooping

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 mld snooping</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td>Step 5</td>
<td>reload</td>
</tr>
</tbody>
</table>

To globally disable MLD snooping on the switch, use the `no ipv6 mld snooping` global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable MLD snooping on a VLAN.

**Note**

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 3560 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 mld snooping</td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 mld snooping vlan vlan-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable MLD snooping on a VLAN interface, use the `no ipv6 mld snooping vlan vlan-id` global configuration command for the specified VLAN number.
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.

Beginning in privileged EXEC mode, follow these steps to add a Layer 2 port as a member of a multicast group:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 mld snooping vlan vlan-id static ipv6_multicast_address interface interface-id</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ipv6 mld snooping multicast-address user</td>
</tr>
<tr>
<td></td>
<td>or show ipv6 mld snooping multicast-address vlan vlan-id user</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove a Layer 2 port from the multicast group, use the no ipv6 mld snooping vlan vlan-id static mac-address interface interface-id global configuration command. If all member ports are removed from a group, the group is deleted.

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

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet0/1
Switch(config)# end
```

Configuring a Multicast Router Port

Although MLD snooping learns about router ports through MLD queries and PIMv6 queries, you can also use the command-line interface (CLI) to add a multicast router port to a VLAN. To add a multicast router port (add a static connection to a multicast router), use the ipv6 mld snooping vlan mrouter global configuration command on the switch.

Note: Static connections to multicast routers are supported only on switch ports.
Beginning in privileged EXEC mode, follow these steps to add a multicast router port to a VLAN:

1. **configure terminal**
   - Purpose: Enter global configuration mode.

2. **ipv6 mld snooping vlan vlan-id mrouter interface interface-id**
   - Specify the multicast router VLAN ID, and specify the interface to the multicast router.
   - The VLAN ID range is 1 to 1001 and 1006 to 4094.
   - The interface can be a physical interface or a port channel.
   - The port-channel range is 1 to 48.

3. **end**
   - Return to privileged EXEC mode.

4. **show ipv6 mld snooping mrouter [vlan vlan-id]**
   - Verify that IPv6 MLD snooping is enabled on the VLAN interface.

5. **copy running-config startup-config**
   - (Optional) Save your entries in the configuration file.

To remove a multicast router port from the VLAN, use the **no ipv6 mld snooping vlan vlan-id mrouter interface interface-id** global configuration command.

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

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config)# exit
```

### Enabling MLD Immediate Leave

When you enable MLDv1 Immediate Leave, the switch immediately removes a port from a multicast group when it detects an MLD Done message on that port. You should only use the Immediate-Leave feature when there is a single receiver present on every port in the VLAN. When there are multiple clients for a multicast group on the same port, you should not enable Immediate-Leave in a VLAN.

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

1. **configure terminal**
   - Purpose: Enter global configuration mode.

2. **ipv6 mld snooping vlan vlan-id immediate-leave**
   - Enable MLD Immediate Leave on the VLAN interface.

3. **end**
   - Return to privileged EXEC mode.

4. **show ipv6 mld snooping vlan vlan-id**
   - Verify that Immediate Leave is enabled on the VLAN interface.

5. **copy running-config startup-config**
   - (Optional) Save your entries in the configuration file.

To disable MLD Immediate Leave on a VLAN, use the **no ipv6 mld snooping vlan vlan-id immediate-leave** global configuration command.

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

When Immediate Leave is not enabled and a port receives an MLD Done message, the switch generates MASQs on the port and sends them to the IPv6 multicast address for which the Done message was sent. You can optionally configure the number of MASQs that are sent and the length of time the switch waits for a response before deleting the port from the multicast group.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ipv6 mld snooping robustness-variable value</td>
</tr>
<tr>
<td>Step 3</td>
<td>ipv6 mld snooping vlan vlan-id robustness-variable value</td>
</tr>
<tr>
<td>Step 4</td>
<td>ipv6 mld snooping last-listener-query-count count</td>
</tr>
<tr>
<td>Step 5</td>
<td>ipv6 mld snooping vlan vlan-id last-listener-query-count count</td>
</tr>
<tr>
<td>Step 6</td>
<td>ipv6 mld snooping last-listener-query-interval interval</td>
</tr>
<tr>
<td>Step 7</td>
<td>ipv6 mld snooping vlan vlan-id last-listener-query-interval interval</td>
</tr>
<tr>
<td>Step 8</td>
<td>ipv6 mld snooping tcn query solicit</td>
</tr>
<tr>
<td>Step 9</td>
<td>ipv6 mld snooping tcn flood query count count</td>
</tr>
<tr>
<td>Step 10</td>
<td>end</td>
</tr>
<tr>
<td>Step 11</td>
<td>show ipv6 mld snooping querier [vlan vlan-id]</td>
</tr>
<tr>
<td>Step 12</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
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
```

**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.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>no ipv6 mld snooping listener-message-suppression</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ipv6 mld snooping</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To re-enable MLD message suppression, use the `ipv6 mld snooping listener-message-suppression` global configuration command.
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 MAC address multicast entries for a VLAN configured for MLD snooping.

To display MLD snooping information, use one or more of the privileged EXEC commands in Table 39-2.

Table 39-2 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>Display the MLD snooping configuration information for all VLANs on the switch or for a specified VLAN. &lt;br&gt; (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>Display 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. &lt;br&gt; (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 querier [vlan vlan-id]</code></td>
<td>Display information about the IPv6 address and incoming port for the most-recently received MLD query messages in the VLAN. &lt;br&gt; (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>`show ipv6 mld snooping multicast-address [vlan vlan-id] [count</td>
<td>dynamic</td>
</tr>
<tr>
<td><code>show ipv6 mld snooping multicast-address vlan vlan-id [ipv6-multicast-address]</code></td>
<td>Display MLD snooping for the specified VLAN and IPv6 multicast address.</td>
</tr>
</tbody>
</table>
Configuring HSRP

This chapter describes how to use Hot Standby Router Protocol (HSRP) on the Catalyst 3560 switch to provide routing redundancy for routing IP traffic not dependent on the availability of any single router. HSRP for IPv4 is supported on switches running the IP base or IP services image. To use HSRP for IPv6, see Chapter 38, “Configuring IPv6 Unicast Routing.”

You can also use a version of HSRP in Layer 2 mode to configure a redundant command switch to take over cluster management if the cluster command switch fails. For more information about clustering, see Chapter 5, “Clustering Switches” and see the Getting Started with Cisco Network Assistant, available on Cisco.com.

For complete syntax and usage information for the commands used in this chapter, see these documents:

- Switch command reference for this release
- Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2:
- Hot Standby Router Protocol Version 2 feature module:

This chapter consists of these sections:

- Understanding HSRP, page 41-1
- Configuring HSRP, page 41-4
- Displaying HSRP Configurations, page 41-13

Understanding HSRP

HSRP is Cisco’s standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.
**Note**

Routers in an HSRP group can be any router interface that supports HSRP, including Catalyst 3560 routed ports and switch virtual interfaces (SVIs).

HSRP provides high network availability by providing redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over the routing duties when an active router fails or when preset conditions are met.

HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new router when their selected router reloads or loses power. When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among router interfaces in a group of router interfaces running HSRP. The router selected by the protocol to be the active router receives and routes packets destined for the group’s MAC address. For \( n \) routers running HSRP, there are \( n + 1 \) IP and MAC addresses assigned.

HSRP detects when the designated active router fails, and a selected standby router assumes control of the Hot Standby group’s MAC and IP addresses. A new standby router is also selected at that time. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. When HSRP is configured on an interface, Internet Control Message Protocol (ICMP) redirect messages are automatically enabled for the interface.

You can configure multiple Hot Standby groups among Catalyst 3560 switches that are operating in Layer 3 to make more use of the redundant routers. To do so, specify a group number for each Hot Standby command group you configure for an interface. For example, you might configure an interface on switch 1 as an active router and one on switch 2 as a standby router and also configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

Figure 41-1 shows a segment of a network configured for HSRP. Each router is configured with the MAC address and IP network address of the virtual router. Instead of configuring hosts on the network with the IP address of Router A, you configure them with the IP address of the virtual router as their default router. When Host C sends packets to Host B, it sends them to the MAC address of the virtual router. If for any reason, Router A stops transferring packets, Router B responds to the virtual IP address and virtual MAC address and becomes the active router, assuming the active router duties. Host C continues to use the IP address of the virtual router to address packets destined for Host B, which Router B now receives and sends to Host B. Until Router A resumes operation, HSRP allows Router B to provide uninterrupted service to users on Host C’s segment that need to communicate with users on Host B’s segment and also continues to perform its normal function of handling packets between the Host A segment and Host B.
HSRP Versions

The switch supports these Hot Standby Redundancy Protocol (HSRP) versions:

- **HSRPv1**—Version 1 of the HSRP, the default version of HSRP. It has these features:
  - The HSRP group number can be from 0 to 255.
  - HSRPv1 uses the multicast address 224.0.0.2 to send hello packets, which can conflict with Cisco Group Management Protocol (CGMP) leave processing. You cannot enable HSRPv1 and CGMP at the same time; they are mutually exclusive.

- **HSRPv2**—Version 2 of the HSRP has these features:
  - To match the HSRP group number to the VLAN ID of a subinterface, HSRPv2 can use a group number from 0 to 4095 and a MAC address from 0000.0C9F.F000 to 0000.0C9F.FFFF.
  - HSRPv2 uses the multicast address 224.0.0.102 to send hello packets. HSRPv2 and CGMP leave processing are no longer mutually exclusive, and both can be enabled at the same time.
  - HSRPv2 has a different packet format than HSRPv1.

A switch running HSRPv1 cannot identify the physical router that sent a hello packet because the source MAC address of the router is the virtual MAC address.

HSRPv2 has a different packet format than HSRPv1. A HSRPv2 packet uses the type-length-value (TLV) format and has a 6-byte identifier field with the MAC address of the physical router that sent the packet.

If an interface running HSRPv1 gets an HSRPv2 packet, the type field is ignored.
Multiple HSRP

The switch supports Multiple HSRP (MHSRP), an extension of HSRP that allows load sharing between two or more HSRP groups. You can configure MHSRP to achieve load balancing and to use two or more standby groups (and paths) from a host network to a server network. In Figure 41-2, half the clients are configured for Router A, and half the clients are configured for Router B. Together, the configuration for Routers A and B establishes two HSRP groups. For group 1, Router A is the default active router because it has the assigned highest priority, and Router B is the standby router. For group 2, Router B is the default active router because it has the assigned highest priority, and Router A is the standby router. During normal operation, the two routers share the IP traffic load. When either router becomes unavailable, the other router becomes active and assumes the packet-transfer functions of the router that is unavailable.

See the “Configuring MHSRP” section on page 41-10 for the example configuration steps.

Note

For MHSRP, you need to enter the `standby preempt` interface configuration command on the HSRP interfaces so that if a router fails and then comes back up, preemption restores load sharing.

Figure 41-2 MHSRP Load Sharing

---

Configuring HSRP

These sections contain this configuration information:

- Default HSRP Configuration, page 41-5
- HSRP Configuration Guidelines, page 41-6
- Enabling HSRP, page 41-6
- Configuring HSRP Priority, page 41-8
Default HSRP Configuration

Table 41-1 shows the default HSRP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSRP version</td>
<td>Version 1</td>
</tr>
<tr>
<td>HSRP groups</td>
<td>None configured</td>
</tr>
<tr>
<td>Standby group number</td>
<td>0</td>
</tr>
<tr>
<td>Standby MAC address</td>
<td>System assigned as: 0000.0c07.acXX, where XX is the HSRP group number</td>
</tr>
<tr>
<td>Standby priority</td>
<td>100</td>
</tr>
<tr>
<td>Standby delay</td>
<td>0 (no delay)</td>
</tr>
<tr>
<td>Standby track interface priority</td>
<td>10</td>
</tr>
<tr>
<td>Standby hello time</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Standby holdtime</td>
<td>10 seconds</td>
</tr>
</tbody>
</table>
HSRP Configuration Guidelines

Follow these guidelines when configuring HSRP:

- HSRP for IPv4 and HSRP for IPv6 are mutually exclusive. You cannot enable both at the same time.
- HSRPv2 and HSRPv1 are mutually exclusive. HSRPv2 is not interoperable with HSRPv1 on an interface and the reverse.
- You can configure up to 32 instances of HSRP groups.

If you configure the same HSRP group number on multiple interfaces, the switch counts each interface as one instance:

For example, if you configure HSRP group 0 on VLAN 1 and on port 1, the switch counts this as two instances.

- In the configuration procedures, the specified interface must be a Layer 3 interface:
  - Routed port: a physical port configured as a Layer 3 port by entering the `no switchport` interface configuration command.
  - SVI: a VLAN interface created by using the `interface vlan vlan_id` global configuration command and by default a Layer 3 interface.
  - EtherChannel port channel in Layer 3 mode: a port-channel logical interface created by using the `interface port-channel port-channel-number` global configuration command and binding the Ethernet interface into the channel group. For more information, see the “Configuring Layer 3 EtherChannels” section.

- All Layer 3 interfaces must have assigned IP addresses. See the “Configuring Layer 3 Interfaces” section on page 11-25 section.
- Configure only one instance of an FHRP. The switches support HSRPv1, HSRPv2, and HSRP for IPv6.
- The version of an HSRP group can be changed from HSRPv2 to HSRPv1 only if the group number is less than 256.
- When configuring group numbers for HSRPv2 and HSRP, you must use group numbers in ranges that are multiples of 256. Valid ranges are 0 to 255, 256 to 511, 512 to 767, 3840 to 4095, and so on.

Examples of valid and invalid group numbers:

- If you configure groups with the numbers 2, 150, and 225, you cannot configure another group with the number 3850. It is not in the range of 0 to 255.
- If you configure groups with the numbers 520, 600, and 700, you cannot configure another group with the number 900. It is not in the range of 512 to 767.
- If you change the HSRP version on an interface, each HSRP group resets because it now has a new virtual MAC address.

Enabling HSRP

The `standby ip` interface configuration command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the address is learned through the standby function. You must configure at least one Layer 3 port on the LAN with the designated address. Configuring an IP address always overrides another designated address currently in use.
When the `standby ip` command is enabled on an interface and proxy ARP is enabled, if the interface’s Hot Standby state is active, proxy ARP requests are answered using the Hot Standby group MAC address. If the interface is in a different state, proxy ARP responses are suppressed.

Beginning in privileged EXEC mode, follow these steps to create or enable HSRP on a Layer 3 interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP.</td>
</tr>
</tbody>
</table>
| 3    | standby version {1 | Configure the HSRP version on the interface.  
|      | 2} (Optional) |  
|      | 1 — Select HSRPv1. |  
|      | 2 — Select HSRPv2. |  
|      | If you do not enter this command or do not specify a keyword, the interface runs the default HSRP version, HSRP v1. |
| 4    | standby [group-number] ip [ip-address [secondary]] | Create (or enable) the HSRP group using its number and virtual IP address.  
|      | 1 — Optional group-number — The group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. |  
|      | 2 — Optional on all but one interface ip-address — The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces. |  
|      | 3 — Optional secondary — The IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router. |  
| 5    | end | Return to privileged EXEC mode. |
| 6    | show standby [interface-id [group]] | Verify the configuration. |
| 7    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the `no standby [group-number] ip [ip-address]` interface configuration command to disable HSRP.

This example shows how to activate HSRP for group 1 on an interface. The IP address used by the hot standby group is learned by using HSRP.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```
Configuring HSRP Priority

The **standby priority**, **standby preempt**, and **standby track** interface configuration commands are all used to set characteristics for finding active and standby routers and behavior regarding when a new active router takes over.

When configuring HSRP priority, follow these guidelines:

- Assigning a priority allows you to select the active and standby routers. If preemption is enabled, the router with the highest priority becomes the active router. If priorities are equal, the current active router does not change.
- The highest number (1 to 255) represents the highest priority (most likely to become the active router).
- When setting the priority, preempt, or both, you must specify at least one keyword (**priority**, **preempt**, or both).
- The priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.
- The **standby track** interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.
- The **standby track interface-priority** interface configuration command specifies how much to decrement the hot standby priority when a tracked interface goes down. When the interface comes back up, the priority is incremented by the same amount.
- When multiple tracked interfaces are down and **interface-priority** values have been configured, the configured priority decrements are cumulative. If tracked interfaces that were not configured with priority values fail, the default decrement is 10, and it is noncumulative.
- When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table.

Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP priority characteristics on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>standby [group-number] priority</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Step 4

Use the `standby [group-number] preempt [delay [minimum seconds]] [reload seconds] [sync seconds]` command to configure the router to preempt, which means that when the local router has a higher priority than the active router, it becomes the active router.

- **(Optional) group-number** — The group number to which the command applies.
- **(Optional) delay minimum** — Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over).
- **(Optional) delay reload** — Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over after a reload).
- **(Optional) delay sync** — Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over).

Use the `no` form of the command to restore the default values.

### Step 5

Configure an interface to track other interfaces so that if one of the other interfaces goes down, the device’s Hot Standby priority is lowered.

- **(Optional) group-number** — The group number to which the command applies.
- **type** — Enter the interface type (combined with interface number) that is tracked.
- **number** — Enter the interface number (combined with interface type) that is tracked.
- **(Optional) interface-priority** — Enter the amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up. The default value is 10.

### Step 6

Return to privileged EXEC mode.

### Step 7

Verify the configuration of the standby groups.

### Step 8

(Optional) Save your entries in the configuration file.

**Command Purpose**

- **Configure the router to preempt**, which means that when the local router has a higher priority than the active router, it becomes the active router.
- **(Optional) group-number** — The group number to which the command applies.
- **(Optional) delay minimum** — Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over).
- **(Optional) delay reload** — Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over after a reload).
- **(Optional) delay sync** — Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an ok or wait reply) for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over).

Use the `no` form of the command to restore the default values.

**Command Purpose**

- **Configure an interface to track other interfaces** so that if one of the other interfaces goes down, the device’s Hot Standby priority is lowered.
- **(Optional) group-number** — The group number to which the command applies.
- **type** — Enter the interface type (combined with interface number) that is tracked.
- **number** — Enter the interface number (combined with interface type) that is tracked.
- **(Optional) interface-priority** — Enter the amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up. The default value is 10.

Use the `no` form of the command to remove the tracking.

This example activates a port, sets an IP address and a priority of 120 (higher than the default value), and waits for 300 seconds (5 minutes) before attempting to become the active router:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
```
Configuring MHSRP

To enable MHSRP and load balancing, you configure two routers as active routers for their groups, with virtual routers as standby routers. This example shows how to enable the MHSRP configuration shown in Figure 41-2. You need to enter the `standby preempt` interface configuration command on each HSRP interface so that if a router fails and comes back up, the preemption occurs and restores load balancing.

Router A is configured as the active router for group 1, and Router B is configured as the active router for group 2. The HSRP interface for Router A has an IP address of 10.0.0.1 with a group 1 standby priority of 110 (the default is 100). The HSRP interface for Router B has an IP address of 10.0.0.2 with a group 2 standby priority of 110.

Group 1 uses a virtual IP address of 10.0.0.3 and group 2 uses a virtual IP address of 10.0.0.4.

**Router A Configuration**

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

**Router B Configuration**

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```
Beginning in privileged EXEC mode, use one or more of these steps to configure HSRP authentication and timers on an interface:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>standby [group-number] authentication string</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>standby [group-number] timers hellotime holdtime</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the **no standby [group-number] authentication string** interface configuration command to delete an authentication string. Use the **no standby [group-number] timers hellotime holdtime** interface configuration command to restore timers to their default values.

This example shows how to configure word as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

This example shows how to set the timers on standby group 1 with the time between hello packets at 5 seconds and the time after which a router is considered down to be 15 seconds:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```
Enabling HSRP Support for ICMP Redirect Messages

The Internet Control Message Protocol (ICMP) is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides diagnostic functions, such as sending and directing error packets to the host.

When the switch is running HSRP, make sure hosts do not discover the interface (or real) MAC addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router and that router later fails, packets from the host will be lost.

The Internet Control Message Protocol (ICMP) is a network layer Internet protocol that provides diagnostic functions, such as sending and directing error packets to the host.

ICMP redirect messages are automatically enabled on interfaces configured with HSRP. This feature filters outgoing ICMP redirect messages through HSRP, in which the next hop IP address might be changed to an HSRP virtual IP address. For more information, see the Cisco IOS IP Configuration Guide, Release 12.2.

Configuring HSRP Groups and Clustering

When a device is participating in an HSRP standby routing and clustering is enabled, you can use the same standby group for command switch redundancy and HSRP redundancy. Use the `cluster standby-group HSRP-group-name [routing-redundancy]` global configuration command to enable the same HSRP standby group to be used for command switch and routing redundancy. If you create a cluster with the same HSRP standby group name without entering the `routing-redundancy` keyword, HSRP standby routing is disabled for the group.

This example shows how to bind standby group my_hsrp to the cluster and enable the same HSRP group to be used for command switch redundancy and router redundancy. The command can only be executed on the cluster command switch. If the standby group name or number does not exist, or if the switch is a cluster member switch, an error message appears.

```
Switch# configure terminal
Switch(config)# cluster standby-group my_hsrp routing-redundancy
Switch(config)# end
```
Troubleshooting HSRP

If one of the situations in Table 41-2 occurs, this message appears:

%FHRP group not consistent with already configured groups on the switch stack - virtual MAC reservation failed

<table>
<thead>
<tr>
<th>Situation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>You configure more than 32 HSRP group instances.</td>
<td>Remove HSRP groups so that up to 32 group instances are configured.</td>
</tr>
<tr>
<td>You configure HSRP for IPv4 and HSRP for IPv6 at the same time</td>
<td>Configure either HSRP for IPv4 or HSRP for IPv6 on the switch.</td>
</tr>
<tr>
<td>You configure group numbers that are not in valid ranges of 256.</td>
<td>Configure group numbers in a valid range.</td>
</tr>
</tbody>
</table>

Displaying HSRP Configurations

From privileged EXEC mode, use this command to display HSRP settings:

`show standby [interface-id [group]] [brief] [detail]`

You can display HSRP information for the whole switch, for a specific interface, for an HSRP group, or for an HSRP group on an interface. You can also specify whether to display a concise overview of HSRP information or detailed HSRP information. The default display is `detail`. If there are a large number of HSRP groups, using the `show standby` command without qualifiers can result in an unwieldy display.

This is an example of output from the `show standby` privileged EXEC command, displaying HSRP information for two standby groups (group 1 and group 100):

Switch# `show standby`

VLAN1 - Group 1
- Local state is Standby, priority 105, may preempt
  Hello time 3 holdtime 10
  Next hello sent in 00:00:02.182
  Hot standby IP address is 172.20.128.3 configured
  Active router is 172.20.128.1 expires in 00:00:09
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac01
  Name is bbb

VLAN1 - Group 100
- Local state is Active, priority 105, may preempt
  Hello time 3 holdtime 10
  Next hello sent in 00:00:02.262
  Hot standby IP address is 172.20.138.51 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac64
  Name is test
This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) on the Catalyst 3560 switch. Cisco IP SLAs is a part of Cisco IOS software that allows Cisco customers to analyze IP service levels for IP applications and services by using active traffic monitoring—the generation of traffic in a continuous, reliable, and predictable manner—for measuring network performance. With Cisco IOS IP SLAs, service provider customers can measure and provide service level agreements, and enterprise customers can verify service levels, verify outsourced service level agreements, and understand network performance. Cisco IOS IP SLAs can perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist with network troubleshooting.

Switches running the IP base image support only IP SLAs responder functionality and must be configured with another device that supports full IP SLAs functionality, for example, a Catalyst 3560 switch running the IP services image.


This chapter has these sections:

- Understanding Cisco IOS IP SLAs, page 42-1
- Configuring IP SLAs Operations, page 42-6
- Monitoring IP SLAs Operations, page 42-14

Understanding Cisco IOS IP SLAs

Cisco IOS IP SLAs sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services and collects network performance information in real time. Cisco IOS IP SLAs generates and analyzes traffic either between Cisco IOS devices or from a Cisco IOS device to a remote IP device such as a network application server. Measurements provided by the various Cisco IOS IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

Depending on the specific Cisco IOS IP SLAs operation, various network performance statistics are monitored within the Cisco device and stored in both command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIBs. IP SLAs packets have configurable IP and application layer
options such as source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), Virtual Private Network (VPN) routing/forwarding instance (VRF), and URL web address.

Because Cisco IP SLAs is Layer 2 transport independent, you can configure end-to-end operations over disparate networks to best reflect the metrics that an end user is likely to experience. IP SLAs collects a unique subset of these performance metrics:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time

Because Cisco IOS IP SLAs is SNMP-accessible, it can also be used by performance-monitoring applications like CiscoWorks Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products. You can find more details about network management products that use Cisco IOS IP SLAs:
http://www.cisco.com/go/ipsla

Using IP SLAs can provide these benefits:

- Service-level agreement monitoring, measurement, and verification.
- Network performance monitoring
  - Measures the jitter, latency, or packet loss in the network.
  - Provides continuous, reliable, and predictable measurements.
- IP service network health assessment to verify that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring for proactive verification and connectivity testing of network resources (for example, shows the network availability of an NFS server used to store business critical data from a remote site).
- Troubleshooting of network operation by providing consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.
- Multiprotocol Label Switching (MPLS) performance monitoring and network verification (if the switch supports MPLS)

This section has this information about IP SLAs functionality:

- Using Cisco IOS IP SLAs to Measure Network Performance, page 42-3
- IP SLAs Responder and IP SLAs Control Protocol, page 42-4
- Response Time Computation for IP SLAs, page 42-4
- IP SLAs Operation Scheduling, page 42-5
- IP SLAs Operation Threshold Monitoring, page 42-5
Using Cisco IOS IP SLAs to Measure Network Performance

You can use IP SLAs to monitor the performance between any area in the network—core, distribution, and edge—without deploying a physical probe. It uses generated traffic to measure network performance between two networking devices. Figure 42-1 shows how IP SLAs begins when the source device sends a generated packet to the destination device. After the destination device receives the packet, depending on the type of IP SLAs operation, it responds with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP.

Figure 42-1 Cisco IOS IP SLAs Operation

To implement IP SLAs network performance measurement, you need to perform these tasks:

1. Enable the IP SLAs responder, if required.
2. Configure the required IP SLAs operation type.
3. Configure any options available for the specified operation type.
4. Configure threshold conditions, if required.
5. Schedule the operation to run, then let the operation run for a period of time to gather statistics.
6. Display and interpret the results of the operation using the Cisco IOS CLI or a network management system (NMS) system with SNMP.

For more information about IP SLAs operations, see the operation-specific chapters in the Cisco IOS IP SLAs Configuration Guide:

Note
The switch does not support Voice over IP (VoIP) service levels using the gatekeeper registration delay operations measurements. Before configuring any IP SLAs application, you can use the show ip sla application privileged EXEC command to verify that the operation type is supported on your software image.
IP SLAs Responder and IP SLAs Control Protocol

The IP SLAs responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without the need for dedicated probes. The responder uses the Cisco IOS IP SLAs Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond. Only a Cisco IOS device can be a source for a destination IP SLAs Responder.

Note

The IP SLAs responder can be a Cisco IOS Layer 2, responder-configurable switch, such as a Catalyst 2960 or IE 3000 switch running the LAN base image, or a Catalyst 3560 or 3750 switch running the IP base image. The responder does not need to support full IP SLAs functionality.

Figure 42-1 shows where the Cisco IOS IP SLAs responder fits in the IP network. The responder listens on a specific port for control protocol messages sent by an IP SLAs operation. Upon receipt of the control message, it enables the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. It disables the port after it responds to the IP SLAs packet, or when the specified time expires. MD5 authentication for control messages is available for added security.

You do not need to enable the responder on the destination device for all IP SLAs operations. For example, a responder is not required for services that are already provided by the destination router (such as Telnet or HTTP). You cannot configure the IP SLAs responder on non-Cisco devices and Cisco IOS IP SLAs can send operational packets only to services native to those devices.

Response Time Computation for IP SLAs

Switches and routers can take tens of milliseconds to process incoming packets due to other high priority processes. This delay affects the response times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimizes these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLAs test packets use time stamping to minimize the processing delays.

When the IP SLAs responder is enabled, it allows the target device to take time stamps when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. This time stamping is made with a granularity of sub-milliseconds (ms).

Figure 42-2 demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target router, with the responder functionality enabled, time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.
Figure 42-2  Cisco IOS IP SLAs Responder Time Stamping

An additional benefit of the two time stamps at the target device is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements, you must configure both the source router and target router with Network Time Protocol (NTP) so that the source and target are synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

IP SLAs Operation Scheduling

When you configure an IP SLAs operation, you must schedule the operation to begin capturing statistics and collecting error information. You can schedule an operation to start immediately or to start at a certain month, day, and hour. You can use the pending option to set the operation to start at a later time. The pending option is an internal state of the operation that is visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

You can schedule several IP SLAs operations on a switch running the IP services image by using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. Scheduling the operations to run at evenly distributed times allows you to control the amount of IP SLAs monitoring traffic. This distribution of IP SLAs operations helps minimize the CPU utilization and thus improves network scalability.


IP SLAs Operation Threshold Monitoring

To support successful service level agreement monitoring, you must have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as these:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
- One-way jitter
- One-way mean opinion score (MOS)
- One-way latency
An IP SLAs threshold violation can also trigger another IP SLAs operation for further analysis. For example, the frequency could be increased or an ICMP path echo or ICMP path jitter operation could be initiated for troubleshooting.

Determining the type of threshold and the level to set can be complex, and depends on the type of IP service being used in the network. For more details on using thresholds with Cisco IOS IP SLAs operations, see the “IP SLAs—Proactive Threshold Monitoring” chapter of the Cisco IOS IP SLAs Configuration Guide:

Configuring IP SLAs Operations

This section does not include configuration information for all available operations as the configuration information details are included in the Cisco IOS IP SLAs Configuration Guide. It does include several operations as examples, including configuring the responder, configuring UDP jitter operation, which requires a responder, and configuring ICMP echo operation, which does not require a responder.

Note
A switch running the IP base image supports only IP SLAs responder functionality. The switch must be running the IP services image for full IP SLAs functionality.

For details about configuring other operations, see the Cisco IOS IP SLAs Configuration Guide:

This section includes this information:

- Default Configuration, page 42-6
- Configuration Guidelines, page 42-6
- Configuring the IP SLAs Responder, page 42-8
- Analyzing IP Service Levels by Using the UDP Jitter Operation, page 42-9
- Analyzing IP Service Levels by Using the ICMP Echo Operation, page 42-12

Default Configuration

No IP SLAs operations are configured.

Configuration Guidelines

For information on the IP SLAs commands, see the Cisco IOS IP SLAs Command Reference, Release 12.4T command reference:

For detailed descriptions and configuration procedures, see the Cisco IOS IP SLAs Configuration Guide, Release 12.4T:
Note that not all of the IP SLAs commands or operations described in this guide are supported on the switch. The switch supports IP service level analysis by using UDP jitter, UDP echo, HTTP, TCP connect, ICMP echo, ICMP path echo, ICMP path jitter, FTP, DNS, and DHCP, as well as multiple operation scheduling and proactive threshold monitoring. It does not support VoIP service levels using the gatekeeper registration delay operations measurements.

Before configuring any IP SLAs application, you can use the `show ip sla application` privileged EXEC command to verify that the operation type is supported on your software image. This is an example of the output from the command:

```
Switch# show ip sla application
IP SLAs
Version: 2.2.0 Round Trip Time MIB, Infrastructure Engine-II
Time of last change in whole IP SLAs: 22:17:39.117 UTC Fri Jun
Estimated system max number of entries: 15801

Estimated number of configurable operations: 15801
Number of Entries configured : 0
Number of active Entries     : 0
Number of pending Entries    : 0
Number of inactive Entries   : 0

Supported Operation Types
Type of Operation to Perform: 802.1agEcho
Type of Operation to Perform: 802.1agJitter
Type of Operation to Perform: dhcp
Type of Operation to Perform: dns
Type of Operation to Perform: echo
Type of Operation to Perform: ftp
Type of Operation to Perform: http
Type of Operation to Perform: jitter
Type of Operation to Perform: pathEcho
Type of Operation to Perform: pathJitter
Type of Operation to Perform: tcpConnect
Type of Operation to Perform: udpEcho

IP SLAs low memory water mark: 21741224
```
Configuring the IP SLAs Responder

The IP SLAs responder is available only on Cisco IOS software-based devices, including some Layer 2 switches that do not support full IP SLAs functionality, such as the Catalyst 2960 or the Cisco ME 2400 or IE 3000 switch running the LAN base image. Beginning in privileged EXEC mode, follow these steps to configure the IP SLAs responder on the target device (the operational target):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip sla responder {tcp-connect</td>
<td>udp-echo</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• tcp-connect—Enable the responder for TCP connect operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• udp-echo—Enable the responder for User Datagram Protocol (UDP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>echo or jitter operations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ipaddress ip-address—Enter the destination IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• port port-number—Enter the destination port number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note The IP address and port number must match those configured on</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the source device for the IP SLAs operation.</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ip sla responder</td>
<td>Verify the IP SLAs responder configuration on the device.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the IP SLAs responder, enter the no ip sla responder global configuration command. This example shows how to configure the device as a responder for the UDP jitter IP SLAs operation in the next procedure:

Switch(config)# ip sla responder udp-echo 172.29.139.134 5000

Note For the IP SLAs responder to function, you must also configure a source device, such as a Catalyst 3750 or Catalyst 3560 switch running the IP services image, that has full IP SLAs support. Refer to the documentation for the source device for configuration information.
Analyzing IP Service Levels by Using the UDP Jitter Operation

Jitter means interpacket delay variance. When multiple packets are sent consecutively 10 ms apart from source to destination, if the network is behaving correctly, the destination should receive them 10 ms apart. But if there are delays in the network (like queuing, arriving through alternate routes, and so on) the arrival delay between packets might be more than or less than 10 ms with a positive jitter value meaning that the packets arrived more than 10 ms apart. If the packets arrive 12 ms apart, positive jitter is 2 ms; if the packets arrive 8 ms apart, negative jitter is 2 ms. For delay-sensitive networks, positive jitter values are undesirable, and a jitter value of 0 is ideal.

In addition to monitoring jitter, the IP SLAs UDP jitter operation can be used as a multipurpose data gathering operation. The packets IP SLAs generates carry packet sending and receiving sequence information and sending and receiving time stamps from the source and the operational target. Based on these, UDP jitter operations measure this data:

- Per-direction jitter (source to destination and destination to source)
- Per-direction packet-loss
- Per-direction delay (one-way delay)
- Round-trip delay (average round-trip time)

Because the paths for the sending and receiving of data can be different (asymmetric), you can use the per-direction data to more readily identify where congestion or other problems are occurring in the network.

The UDP jitter operation generates synthetic (simulated) UDP traffic and sends a number of UDP packets, each of a specified size, sent a specified number of milliseconds apart, from a source router to a target router, at a given frequency. By default, ten packet-frames, each with a payload size of 10 bytes are generated every 10 ms, and the operation is repeated every 60 seconds. You can configure each of these parameters to best simulate the IP service you want to provide.

To provide accurate one-way delay (latency) measurements, time synchronization, such as that provided by NTP, is required between the source and the target device. Time synchronization is not required for the one-way jitter and packet loss measurements. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data is returned, but values of 0 are returned for the one-way delay measurements provided by the UDP jitter operation.

### Note
Before you configure a UDP jitter operation on the source device, you must enable the IP SLAs responder on the target device (the operational target).
Beginning in privileged EXEC mode, follow these steps to configure UDP jitter operation on the source device:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip sla operation-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>udp-jitter {destination-ip-address</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></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>frequency seconds</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
</tr>
</tbody>
</table>
To disable the IP SLAs operation, enter the no ip sla operation-number global configuration command. This example shows how to configure a UDP jitter IP SLAs operation:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# udp-jitter 172.29.139.134 5000
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 10
```

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled

**Command** | **Purpose**
---|---
**Step 6** | **ip sla monitor schedule**<br>operation-number [life {forever | seconds}] [start-time {hh:mm:ss} [month day] | pending | now | after hh:mm:ss] [ageout seconds] [recurring]
| Configure the scheduling parameters for an individual IP SLAs operation.<br>• **operation-number**—Enter the RTR entry number.<br>• (Optional) **life**—Set the operation to run indefinitely (forever) or for a specific number of seconds. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).<br>• (Optional) **start-time**—Enter the time for the operation to begin collecting information:<br>  – To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.<br>  – Enter **pending** to select no information collection until a start time is selected.<br>  – Enter **now** to start the operation immediately.<br>  – Enter **after hh:mm:ss** to show that the operation should start after the entered time has elapsed.<br>• (Optional) **ageout seconds**—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds, the default is 0 seconds (never ages out).<br>• (Optional) **recurring**—Set the operation to automatically run every day.
**Step 7** | **end**
| Return to privileged EXEC mode.
**Step 8** | **show ip sla configuration** [operation-number]
| (Optional) Display configuration values, including all defaults for all IP SLAs operations or a specified operation.
**Step 9** | **copy running-config startup-config**
| (Optional) Save your entries in the configuration file.
Analyzing IP Service Levels by Using the ICMP Echo Operation

The ICMP echo operation measures end-to-end response time between a Cisco device and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP echo request message to the destination and receiving an ICMP echo reply. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements between the source IP SLAs device and the destination IP device. The IP SLAs ICMP echo operation conforms to the same specifications as ICMP ping testing, and the two methods result in the same response times.

**Note**

This operation does not require the IP SLAs responder to be enabled.

Beginning in privileged EXEC mode, follow these steps to configure an ICMP echo operation on the source device:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip sla operation-number Create an IP SLAs operation and enter IP SLAs configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>icmp-echo [destination-ip-address] [destination-hostname] [source-ip] [ip-address</td>
</tr>
<tr>
<td></td>
<td>• destination-ip-address</td>
</tr>
<tr>
<td></td>
<td>• (Optional) source-ip [ip-address</td>
</tr>
<tr>
<td></td>
<td>• (Optional) source-interface interface-id—Specify the source interface for the operation.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>frequency seconds (Optional) Set the rate at which a specified IP SLAs operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit Exit UDP jitter configuration mode, and return to global configuration mode.</td>
</tr>
</tbody>
</table>
To disable the IP SLAs operation, enter the `no ip sla operation-number` global configuration command. This example shows how to configure an ICMP echo IP SLAs operation:

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 172.29.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.
```

Entry number: 12
Owner: 
Tag: 
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Monitoring IP SLAs Operations

Use the User EXEC or Privileged EXEC commands in Table 42-1 to display IP SLAs operations configuration and results.

Table 42-1 Monitoring IP SLAs Operations

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip sla application</td>
<td>Display global information about Cisco IOS IP SLAs.</td>
</tr>
<tr>
<td>show ip sla authentication</td>
<td>Display IP SLAs authentication information.</td>
</tr>
<tr>
<td>show ip sla configuration [entry-number]</td>
<td>Display configuration values including all defaults for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td>show ip sla enhanced-history {collection-statistics</td>
<td>distribution statistics} [entry-number]</td>
</tr>
<tr>
<td>show ip sla ethernet-monitor configuration [entry-number]</td>
<td>Display IP SLAs automatic Ethernet configuration.</td>
</tr>
<tr>
<td>show ip sla group schedule [schedule-entry-number]</td>
<td>Display IP SLAs group scheduling configuration and details.</td>
</tr>
<tr>
<td>show ip sla history [entry-number</td>
<td>full</td>
</tr>
<tr>
<td>show ip sla mpls-lsp-monitor {collection-statistics</td>
<td>configuration</td>
</tr>
<tr>
<td>show ip sla reaction-configuration [entry-number]</td>
<td>Display the configured proactive threshold monitoring settings for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td>show ip sla reaction-trigger [entry-number]</td>
<td>Display the reaction trigger information for all IP SLAs operations or a specific operation.</td>
</tr>
<tr>
<td>show ip sla responder</td>
<td>Display information about the IP SLAs responder.</td>
</tr>
<tr>
<td>show ip sla statistics [entry-number</td>
<td>aggregated</td>
</tr>
</tbody>
</table>
Configuring Enhanced Object Tracking

This chapter describes how to configure enhanced object tracking on the Catalyst 3560 switch. This feature provides a more complete alternative to the Hot Standby Routing Protocol (HSRP) tracking mechanism, which allows you to track the line-protocol state of an interface. If the line protocol state of an interface goes down, the HSRP priority of the interface is reduced and another HSRP device with a higher priority becomes active. The enhanced object tracking feature separates the tracking mechanism from HSRP and creates a separate, standalone tracking process that can be used by processes other than HSRP. This allows tracking other objects in addition to the interface line-protocol state. A client process, such as HSRP, can register an interest in tracking objects and request notification when the tracked object changes state. This feature increases the availability and speed of recovery of a routing system and decreases outages and outage duration.

For more information about enhanced object tracking and the commands used to configure it: http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_eot.html

The chapter has these sections:

- Understanding Enhanced Object Tracking, page 43-1
- Configuring Enhanced Object Tracking Features, page 43-1
- Monitoring Enhanced Object Tracking, page 43-13

Understanding Enhanced Object Tracking

Each tracked object has a unique number that is specified in the tracking command-line interface (CLI). Client processes use this number to track a specific object. The tracking process periodically polls the tracked object for value changes and sends any changes (as up or down values) to interested client processes, either immediately or after a specified delay. Several clients can track the same object, and can take different actions when the object changes state.

You can also track a combination of objects in a list by using either a weight threshold or a percentage threshold to measure the state of the list. You can combine objects using Boolean logic. A tracked list with a Boolean “AND” function requires that each object in the list be in an up state for the tracked object to be up. A tracked list with a Boolean “OR” function needs only one object in the list to be in the up state for the tracked object to be up.

Configuring Enhanced Object Tracking Features

These sections describe configuring enhanced object tracking:
### Default Configuration

No type of object tracking is configured.

### Tracking Interface Line-Protocol or IP Routing State

You can track either the interface line protocol state or the interface IP routing state. When you track the IP routing state, these three conditions are required for the object to be up:

- IP routing must be enabled and active on the interface.
- The interface line-protocol state must be up.
- The interface IP address must be known.

If all three of these conditions are not met, the IP routing state is down.

Beginning in privileged EXEC mode, follow these steps to track the line-protocol state or IP routing state of an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>track object-number interface interface-id line-protocol</td>
<td>(Optional) Create a tracking list to track the line-protocol state of an interface and enter tracking configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The object-number identifies the tracked object and can be from 1 to 500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The interface interface-id is the interface being tracked.</td>
</tr>
<tr>
<td>3</td>
<td>delay {up seconds [down seconds]</td>
<td>{up seconds} down seconds}</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>track object-number interface interface-id ip routing</td>
<td>(Optional) Create a tracking list to track the IP routing state of an interface, and enter tracking configuration mode. IP-route tracking tracks an IP route in the routing table and the ability of an interface to route IP packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The object-number identifies the tracked object and can be from 1 to 500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The interface interface-id is the interface being tracked.</td>
</tr>
<tr>
<td>6</td>
<td>delay {up seconds [down seconds]</td>
<td>{up seconds} down seconds}</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
This example configures the tracking of an interface line-protocol state and verifies the configuration:

```
Switch(config)# track 33 interface gigabitethernet 0/1 line-protocol
Switch(config)# track 33 interface gigabitethernet 1/1 line-protocol
Switch(config-track)# end
Switch# show track 33
Track 33
  Interface GigabitEthernet0/1 line-protocol
  Line protocol is Down (hw down)
  1 change, last change 00:18:28
```

### Configuring a Tracked List

You can configure a tracked list of objects with a Boolean expression, a weight threshold, or a percentage threshold. A tracked list contains one or more objects. An object must exist before it can be added to the tracked list.

- You configure a Boolean expression to specify calculation by using either “AND” or “OR” operators.
- When you measure the tracked list state by a weight threshold, you assign a weight number to each object in the tracked list. The state of the tracked list is determined by whether or not the threshold was met. The state of each object is determined by comparing the total weight of all objects against a threshold weight for each object.
- When you measure the tracked list by a percentage threshold, you assign a percentage threshold to all objects in the tracked list. The state of each object is determined by comparing the assigned percentages of each object to the list.

### Configuring a Tracked List with a Boolean Expression

Configuring a tracked list with a Boolean expression enables calculation by using either “AND” or “OR” operators. For example, when tracking two interfaces using the “AND” operator, *up* means that both interfaces are up, and *down* means that either interface is down.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show track object-number</td>
<td>Verify that the specified objects are being tracked.</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to configure a tracked list of objects with a Boolean expression:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track track-number list boolean { and</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>object object-number [not]</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>delay { up seconds [down seconds] }</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show track object-number</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no track track-number global configuration command to delete the tracked list.

This example configures track list 4 with a Boolean AND expression that contains two objects with one object state negated. If the list is up, the list detects that object 2 is down:

```
Switch(config)# track 4 list boolean and
Switch(config-track)# object 1
Switch(config-track)# object 2 not
Switch(config-track)# exit
```

**Configuring a Tracked List with a Weight Threshold**

To track by weight threshold, configure a tracked list of objects, specify that weight is used as the threshold, and configure a weight for each of its objects. The state of each object is determined by comparing the total weight of all objects that are up against a threshold weight for each object.

You cannot use the Boolean “NOT” operator in a weight threshold list.
Beginning in privileged EXEC mode, follow these steps to configure a tracked list of objects by using a weight threshold and to configure a weight for each object:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>track track-number list threshold weight</td>
</tr>
<tr>
<td></td>
<td>• threshold—Specify the state of the tracked list based on a threshold.</td>
</tr>
<tr>
<td></td>
<td>• weight—Specify that the threshold is based on weight.</td>
</tr>
<tr>
<td>Step 3</td>
<td>object object-number [weight weight-number]</td>
</tr>
<tr>
<td></td>
<td>Note An object must exist before you can add it to a tracked list.</td>
</tr>
<tr>
<td>Step 4</td>
<td>threshold weight {up number</td>
</tr>
<tr>
<td></td>
<td>• up number—The valid range is from 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>• down number—(Optional) The range depends on the number selected for the up number. If you configure the up number as 25, the range shown for the down number is 0 to 24.</td>
</tr>
<tr>
<td>Step 5</td>
<td>delay {up seconds [down seconds]</td>
</tr>
<tr>
<td></td>
<td>[up seconds] down seconds}</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show track object-number</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no track track-number global configuration command to delete the tracked list.

The example configures track list 4 to track by weight threshold. If object 1 and object 2 are down, then track list 4 is up because object 3 satisfies the up threshold value of up 30. But if object 3 is down, both objects 1 and 2 must be up in order to satisfy the threshold weight.

Switch(config)# track 4 list threshold weight
Switch(config-track)# object 1 weight 15
Switch(config-track)# object 2 weight 20
Switch(config-track)# object 3 weight 30
Switch(config-track)# threshold weight up 30 down 10
Switch(config-track)# exit

This configuration can be useful if object 1 and object 2 represent two small bandwidth connections and object 3 represents one large bandwidth connection. The configured down 10 value means that once the tracked object is up, it will not go down until the threshold value is equal to or lower than 10, which in this example means that all connections are down.

**Configuring a Tracked List with a Percentage Threshold**

To track by percentage threshold, configure a tracked list of objects, specify that a percentage will be used as the threshold, and specify a percentage for each object in the list. The state of the list is determined by comparing the assigned percentage of each object to the list.

You cannot use the Boolean “NOT” operator in a percentage threshold list.
Beginning in privileged EXEC mode, follow these steps to configure a tracked list of objects by using a percentage threshold:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
configure terminal | Enter global configuration mode. |
| **Step 2**
track track-number list threshold percentage | Configure a tracked list object and enter tracking configuration mode. The *track-number* can be from 1 to 500.
- **threshold**—Specify the state of the tracked list based on a threshold.
- **percentage**—Specify that the threshold is based on percentage. |
| **Step 3**
object object-number | Specify the object to be tracked. The range is from 1 to 500.
*Note* An object must exist before you can add it to a tracked list. |
| **Step 4**
threshold percentage \{ up number \[ down number \]} | Specify the threshold percentage.
- **up number**—The valid range is from 1 to 100.
- **down number**—(Optional) The range depends on the number selected for the **up number**. If you configure the **up number** as 25, the range shown for the down number is 0 to 24. |
| **Step 5**
delay \{ up seconds \[ down seconds \]} \[ up seconds \]down seconds \} | (Optional) Specify a period of time in seconds to delay communicating state changes of a tracked object. The range is from 1 to 180 seconds. |
| **Step 6**
end | Return to privileged EXEC mode. |
| **Step 7**
show track object-number | Verify that the specified objects are being tracked. |
| **Step 8**
copy running-config startup-config | (Optional) Save your entries in the configuration file. |

Use the **no track track-number** global configuration command to delete the tracked list.

This example configures tracked list 4 with three objects and a specified percentages to measure the state of the list:

```plaintext
Switch(config)# track 4 list threshold percentage
Switch(config-track)# object 1
Switch(config-track)# object 2
Switch(config-track)# object 3
Switch(config-track)# threshold percentage up 51 down 10
Switch(config-track)# exit
```
Configuring HSRP Object Tracking

Beginning in privileged EXEC mode, follow these steps to configure a standby HSRP group to track an object and change the HSRP priority based on the object state:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track object-number {interface interface-id [line-protocol</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>standby [group-number] ip [ip-address [secondary]]</td>
</tr>
</tbody>
</table>

(Optional) Create a tracking list to track the configured state and enter tracking configuration mode.

- The *object-number* range is from 1 to 500.
- Enter *interface* *interface-id* to select an interface to track.
- Enter *line-protocol* to track the interface line protocol state or enter *ip routing* to track the interface IP routing state.
- Enter *ip route* *ip-address/prefix-length* to track the state of an IP route.
- Enter *metric threshold* to track the threshold metric or enter *reachability* to track if the route is reachable.

The default up threshold is 254 and the default down threshold is 255.

- Enter *list* to track objects grouped in a list. Configure the list as described on the previous pages.
  - For *boolean*, see the “Configuring a Tracked List with a Boolean Expression” section on page 43-3
  - For *threshold weight*, see the “Configuring a Tracked List with a Weight Threshold” section on page 43-4
  - For *threshold percentage*, see the “Configuring a Tracked List with a Percentage Threshold” section on page 43-5

**Note** Repeat this step for each interface to be tracked.

(Optional) Create (or enable) the HSRP group by using its number and virtual IP address.

- (Optional) *group-number*—Enter a group number on the interface for which HSRP is being enabled. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number.
- (Optional on all but one interface) *ip-address*—Specify the virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.
- (Optional) *secondary*—Specify that the IP address is a secondary hot standby router interface. If this keyword is omitted, the configured address is the primary IP address.
Configuring Other Tracking Characteristics

You can also use the enhanced object tracking for tracking other characteristics.

- You can track the reachability of an IP route by using the `track ip route reachability` global configuration command.
- You can use the `track ip route metric threshold` global configuration command to determine if a route is above or below threshold.
- You can use the `track resolution` global configuration command to change the metric resolution default values for routing protocols.
- You can use the `track timer` tracking configuration command to configure the tracking process to periodically poll tracked objects.

Use the `show track` privileged EXEC command to verify enhanced object tracking configuration.

For more information about enhanced object tracking and the commands used to configure it:

Configuring IP SLAs Object Tracking

Cisco IOS IP Service Level Agreements (IP SLAs) is a network performance measurement and diagnostics tool that uses active monitoring by generating traffic to measure network performance. Cisco IP SLAs operations collects real-time metrics that you can use for network troubleshooting, design, and analysis.

For more information about Cisco IP SLAs on the switch, see Chapter 42, “Configuring Cisco IOS IP SLAs Operations.” For IP SLAs command information see the Cisco IOS IP SLAs Command Reference, Release 12.4T:

Object tracking of IP SLAs operations allows clients to track the output from IP SLAs objects and use this information to trigger an action. Every IP SLAs operation maintains an SNMP operation return-code value, such as OK or OverThreshold, that can be interpreted by the tracking process. You can track two

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>standby [group-number] track object-number [decrement [priority-decrement]]</code></td>
<td>Configure HSRP to track an object and change the hot standby priority based on the state of the object.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) <code>group-number</code>—Enter the group number to which the tracking applies.</td>
</tr>
<tr>
<td></td>
<td>- <code>object-number</code>—Enter a number representing the object to be tracked. The range is from 1 to 500; the default is 1.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) <code>decrement priority-decrement</code>—Specify the amount by which the hot standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up). The range is from 1 to 255; the default is 10.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><code>standby [group-number] track object-number [decrement [priority-decrement]]</code></td>
<td>Configure HSRP to track an object and change the hot standby priority based on the state of the object.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) <code>group-number</code>—Enter the group number to which the tracking applies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>object-number</code>—Enter a number representing the object to be tracked. The range is from 1 to 500; the default is 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- (Optional) <code>decrement priority-decrement</code>—Specify the amount by which the hot standby priority for the router is decremented (or incremented) when the tracked object goes down (or comes back up). The range is from 1 to 255; the default is 10.</td>
</tr>
<tr>
<td>7</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td><code>show standby</code></td>
<td>Verify the standby router IP address and tracking states.</td>
</tr>
<tr>
<td>9</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
aspects of IP SLAs operation: state and reachability. For state, if the return code is OK, the track state is up; if the return code is not OK, the track state is down. For reachability, if the return code is OK or OverThreshold, reachability is up; if not OK, reachability is down.

Beginning in privileged EXEC mode, follow these steps to track the state of an IP SLAs operation or the reachability of an IP SLAs IP host:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>track object-number rtr operation-number state</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>delay {up seconds [down seconds]</td>
</tr>
<tr>
<td></td>
<td>[up seconds] down seconds}</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>track object-number rtr operation-number reachability</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>delay {up seconds [down seconds]</td>
</tr>
<tr>
<td></td>
<td>[up seconds] down seconds}</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show track object-number</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

This example shows how to configure and display IP SLAs state tracking:

```
Switch(config)# track 2 200 state
Switch(config)# end
Switch# show track 2
Track 2
 Response Time Reporter 1 state
   State is Down
   1 change, last change 00:00:47
 Latest operation return code: over threshold
 Latest RTT (milliseconds) 4
 Tracked by:
   HSRP Ethernet0/1 3
```

This example output shows whether a route is reachable:

```
Switch(config)# track 3 500 reachability
Switch(config)# end
Switch# show track 3
Track 3
 Response Time Reporter 1 reachability
 Reachability is Up
   1 change, last change 00:00:47
 Latest operation return code: over threshold
 Latest RTT (milliseconds) 4
 Tracked by:
   HSRP Ethernet0/1 3
```
Configuring Static Routing Support

Switches that are running the IP services image with Cisco IOS release 12.2(46)SE or later support enhanced object tracking static routing. Static routing support using enhanced object tracking provides the ability for the switch to use ICMP pings to identify when a preconfigured static route or a DHCP route goes down. When tracking is enabled, the system tracks the state of the route and informs the client when that state changes. Static route object tracking uses Cisco IP SLAs to generate ICMP pings to monitor the state of the connection to the primary gateway.

- For more information about Cisco IP SLAs support on the switch, see Chapter 42, “Configuring Cisco IOS IP SLAs Operations.”
- For more information about static route object tracking:

You use this process to configure static route object tracking:

### Step 1
Configure a primary interface for static routing or for DHCP.

### Step 2
Configure an IP SLAs agent to ping an IP address using a primary interface and a track object to monitor the state of the agent.

### Step 3
Configure a default static default route using a secondary interface. This route is used only if the primary route is removed.

### Configuring a Primary Interface

Beginning in privileged EXEC mode, follow these steps to configure a primary interface for static routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Select a primary or secondary interface and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 description string</td>
<td>Add a description to the interface.</td>
</tr>
<tr>
<td>Step 4 ip address ip-address mask [secondary]</td>
<td>Set the primary or secondary IP address for the interface.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
</tr>
</tbody>
</table>

Beginning in privileged EXEC mode, follow these steps to configure a primary interface for DHCP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Select a primary or secondary interface and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 description string</td>
<td>Add a description to the interface.</td>
</tr>
<tr>
<td>Step 4 ip dhcp client route track number</td>
<td>Configure the DCHP client to associate any added routes with the specified track number. Valid numbers are from 1 to 500.</td>
</tr>
</tbody>
</table>
### Configuring a Cisco IP SLAs Monitoring Agent and Track Object

Beginning in privileged EXEC mode, follow these steps to configure network monitoring with Cisco IP SLAs:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip sla operation-number</td>
<td>Begin configuring a Cisco IP SLAs operation and enter IP SLA configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-echo {destination-ip-address</td>
<td>Configure a Cisco IP SLAs end-to-end ICMP echo response time operation and enter IP SLAs ICMP echo configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>
| destination hostname [source-ipaddr | \{ip-address | hostname source-interface interface-id]

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout milliseconds</td>
<td>Set the amount of time for which the operation waits for a response from its request packet.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency seconds</td>
<td>Set the rate at which the operation is sent into the network.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold milliseconds</td>
<td>Set the rising threshold (hysteresis) that generates a reaction event and stores history information for the operation.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exit IP SLAs ICMP echo configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip sla schedule operation-number {life</td>
<td>Configure the scheduling parameters for a single IP SLAs operation.</td>
<td></td>
</tr>
</tbody>
</table>
| \{forever | seconds\}] start-time time | \{pending | now | after \} [ageout \{seconds\}] [recurring]

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>track object-number rtr operation-number</td>
<td>Track the state of a Cisco IOS IP SLAs operation and enter tracking configuration mode.</td>
<td></td>
</tr>
<tr>
<td>{state</td>
<td>reachability}</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show track object-number</td>
<td>Display tracking information to verify the configuration.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring a Routing Policy and Default Route

Beginning in privileged EXEC mode, follow these steps to configure a routing policy for backup static routing by using object tracking. For more details about the commands in the procedure:  

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>access-list</code> access-list-number</td>
<td>Define an extended IP access list. Configure any optional characteristics.</td>
</tr>
<tr>
<td>3</td>
<td><code>route-map</code> map-tag [permit</td>
<td>deny] [sequence-number]</td>
</tr>
<tr>
<td>4</td>
<td><code>match ip address</code> access-list number</td>
<td>Distribute any routes that have a destination network number address that is permitted by a standard or extended access list or performs policy routing on packets. You can enter multiple numbers or names.</td>
</tr>
<tr>
<td>5</td>
<td><code>set ip next-hop dynamic dhcp</code></td>
<td>For DHCP networks only. Set the next hop to the gateway that was most recently learned by the DHCP client.</td>
</tr>
<tr>
<td>6</td>
<td><code>set interface</code> interface-id</td>
<td>For static routing networks only. Indicate where to send output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>7</td>
<td><code>exit</code></td>
<td>Exit route-map configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td><code>ip local policy route-map</code> map-tag</td>
<td>Identify a route map to use for local policy routing.</td>
</tr>
<tr>
<td>9</td>
<td><code>ip route</code> prefix mask ip-address [interface-id ip-address]] [distance name] [permanent</td>
<td>track track-number] [tag tag]</td>
</tr>
<tr>
<td>10</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>11</td>
<td><code>show ip route track table</code></td>
<td>Display information about the IP route track table.</td>
</tr>
<tr>
<td>12</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Monitoring Enhanced Object Tracking

Use the privileged EXEC or User EXEC commands in Table 43-1 to display enhanced object tracking information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip route track table</td>
<td>Display information about the IP route track table.</td>
</tr>
<tr>
<td>show track [object-number]</td>
<td>Display information about the all tracking lists or the specified list.</td>
</tr>
<tr>
<td>show track brief</td>
<td>Display a single line of tracking information output.</td>
</tr>
<tr>
<td>show track interface [brief]</td>
<td>Display information about tracked interface objects.</td>
</tr>
<tr>
<td>show track ip [object-number] [brief] route</td>
<td>Display information about tracked IP-route objects.</td>
</tr>
<tr>
<td>show track resolution</td>
<td>Display the resolution of tracked parameters.</td>
</tr>
<tr>
<td>show track timers</td>
<td>Display tracked polling interval timers.</td>
</tr>
</tbody>
</table>
Configuring Cache Services By Using WCCP

This chapter describes how to configure your Catalyst 3560 switch to redirect traffic to wide-area application engines (such as the Cisco Cache Engine 550) by using the Web Cache Communication Protocol (WCCP). This software release supports only WCCP version 2 (WCCPv2).

WCCP is a Cisco-developed content-routing technology that you can use to integrate wide-area application engines—referred to as application engines—into your network infrastructure. The application engines transparently store frequently accessed content and then fulfill successive requests for the same content, eliminating repetitive transmissions of identical content from servers. Application engines accelerate content delivery and ensure maximum scalability and availability of content. In a service-provider network, you can deploy the WCCP and application engine solution at the points of presence (POPs). In an enterprise network, you can deploy the WCCP and application engine solution at the regional site and the small branch office.

To use this feature, the switch must be running the IP services image.

For complete syntax and usage information for the commands used in this chapter, see the “WCCP Router Configuration Commands” section in the “System Management Commands” part of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*. Access this document from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Understanding WCCP, page 44-1
- Configuring WCCP, page 44-5
- Monitoring and Maintaining WCCP, page 44-9

Understanding WCCP

The WCCP and Cisco cache engines (or other application engines running WCCP) localize traffic patterns in the network, enabling content requests to be fulfilled locally.

WCCP enables supported Cisco routers and switches to transparently redirect content requests. With transparent redirection, users do not have to configure their browsers to use a web proxy. Instead, they can use the target URL to request content, and their requests are automatically redirected to an application engine. The word *transparent* means that the end user does not know that a requested file (such as a web page) came from the application engine instead of from the originally specified server.
When an application engine receives a request, it attempts to service it from its own local cache. If the requested information is not present, the application engine sends a separate request to the end server to retrieve the requested information. After receiving the requested information, the application engine forwards it to the requesting client and also caches it to fulfill future requests.

With WCCP, the application-engine cluster (a series of application engines) can service multiple routers or switches, as shown Figure 44-1.

Figure 44-1  Cisco Cache Engine and WCCP Network Configuration

WCCP Message Exchange

This sequence of events describes the WCCP message exchange:

1. The application engines send their IP addresses to the WCCP-enabled switch by using WCCP, signaling their presence through a Here I am message. The switch and application engines communicate to each other through a control channel based on UDP port 2048.

2. The WCCP-enabled switch uses the application engine IP information to create a cluster view (a list of application engines in the cluster). This view is sent through an I see you message to each application engine in the cluster, essentially making all the application engines aware of each other. A stable view is established after the membership of the cluster remains the same for a certain amount of time.

3. When a stable view is established, the application engine in the cluster with the lowest IP address is elected as the designated application engine.
WCCP Negotiation

In the exchange of WCCP protocol messages, the designated application engine and the WCCP-enabled switch negotiate these items:

- Forwarding method (the method by which the switch forwards packets to the application engine). The switch rewrites the Layer 2 header by replacing the packet destination MAC address with the target application engine MAC address. It then forwards the packet to the application engine. This forwarding method requires the target application engine to be directly connected to the switch at Layer 2.

- Assignment method (the method by which packets are distributed among the application engines in the cluster). The switch uses some bits of the destination IP address, the source IP address, the destination Layer 4 port, and the source Layer 4 port to determine which application engine receives the redirected packets.

- Packet-return method (the method by which packets are returned from the application engine to the switch for normal forwarding). These are the typical reasons why an application engine rejects packets and starts the packet-return feature:
  - The application engine is overloaded and has no room to service the packets.
  - The application engine receives an error message (such as a protocol or authentication error) from the server and uses the dynamic client bypass feature. The bypass enables clients to bypass the application engines and to connect directly to the server.

The application engine returns a packet to the WCCP-enabled switch to forward to the server as if the application engine is not present. The application engine does not intercept the reconnection attempt. In this way, the application engine effectively cancels the redirection of a packet to the application engine and creates a bypass flow. If the return method is generic-route encapsulation (GRE), the switch receives the returned packet through a GRE tunnel that is configured in the application engine. The switch CPU uses Cisco Express Forwarding to send these packets to the target server. If the return method is Layer 2 rewrite, the packets are forwarded in hardware to the target server. When the server responds with the information, the switch uses normal Layer 3 forwarding to return the information to the requesting client.

MD5 Security

WCCP provides an optional security component in each protocol message to enable the switch to use MD5 authentication on messages between the switch and the application engine. Messages that do not authenticate by MD5 (when authentication of the switch is enabled) are discarded by the switch. The password string is combined with the MD5 value to create security for the connection between the switch and the application engine. You must configure the same password on each application engine.

Packet Redirection and Service Groups

You can configure WCCP to classify traffic for redirection, such as FTP, proxy-web-cache handling, and audio and video applications. This classification, known as a service group, is based on the protocol type (TCP or UDP) and the Layer 4 source destination port numbers. The service groups are identified either by well-known names such as web-cache, which means TCP port 80, or a service number, 0 to 99. Service groups are configured to map to a protocol and Layer 4 port numbers and are established and maintained independently. WCCP allows dynamic service groups, where the classification criteria are provided dynamically by a participating application engine.
Understanding WCCP

You can configure up to 8 service groups on a switch or switch stack and up to 32 cache engines per service group. WCCP maintains the priority of the service group in the group definition. WCCP uses the priority to configure the service groups in the switch hardware. For example, if service group 1 has a priority of 100 and looks for destination port 80, and service group 2 has a priority of 50 and looks for source port 80, the incoming packet with source and destination port 80 is forwarded by using service group 1 because it has the higher priority.

WCCP supports a cluster of application engines for every service group. Redirected traffic can be sent to any one of the application engines. The switch supports the mask assignment method of load balancing the traffic among the application engines in the cluster for a service group.

After WCCP is configured on the switch, the switch forwards all service group packets received from clients to the application engines. However, these packets are not redirected:

- Packets originating from the application engine and targeted to the server.
- Packets originating from the application engine and targeted to the client.
- Packets returned or rejected by the application engine. These packets are sent to the server.

You can configure a single multicast address per service group for sending and receiving protocol messages. When there is a single multicast address, the application engine sends a notification to one address, which provides coverage for all routers in the service group, for example, 225.0.0.0. If you add and remove routers dynamically, using a single multicast address provides easier configuration because you do not need to specifically enter the addresses of all devices in the WCCP network.

You can use a router group list to validate the protocol packets received from the application engine. Packets matching the address in the group list are processed, packets not matching the group list address are dropped.

To disable caching for specific clients, servers, or client/server pairs, you can use a WCCP redirect access control list (ACL). Packets that do not match the redirect ACL bypass the cache and are forwarded normally.

Before WCCP packets are redirected, the switch examines ACLs associated with all inbound features configured on the interface and permits or denies packet forwarding based on how the packet matches the entries in the ACL.

Note

Only permit ACL entries are supported in WCCP redirect lists.

When packets are redirected, the output ACLs associated with the redirected interface are applied to the packets. Any ACLs associated with the original port are not applied unless you specifically configure the required output ACLs on the redirected interfaces.

Unsupported WCCP Features

These WCCP features are not supported in this software release:

- Packet redirection on an outbound interface that is configured by using the ip wccp redirect out interface configuration command. This command is not supported.
- The GRE forwarding method for packet redirection is not supported.
- The hash assignment method for load balancing is not supported.
- There is no SNMP support for WCCP.
Configuring WCCP

These sections describe how to configure WCCP on your switch:

- Default WCCP Configuration, page 44-5
- WCCP Configuration Guidelines, page 44-5
- Enabling the Cache Service, page 44-6 (required)

Default WCCP Configuration

Table 44-1 shows the default WCCP configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCCP enable state</td>
<td>WCCP services are disabled.</td>
</tr>
<tr>
<td>Protocol version</td>
<td>WCCPv2.</td>
</tr>
<tr>
<td>Redirecting traffic received on an interface</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

WCCP Configuration Guidelines

Before configuring WCCP on your switch, make sure to follow these configuration guidelines:

- The application engines and switches in the same service group must be in the same subnetwork directly connected to the switch that has WCCP enabled.
- Configure the switch interfaces that are connected to the clients, the application engines, and the server as Layer 3 interfaces (routed ports and switch virtual interfaces [SVIs]). For WCCP packet redirection to work, the servers, application engines, and clients must be on different subnets.
- Use only nonreserved multicast addresses when configuring a single multicast address for each application engine.
- WCCP entries and PBR entries use the same TCAM region. WCCP is supported only on the templates that support PBR: access, routing, and dual IPv4/v6 routing.
- When TCAM entries are not available to add WCCP entries, packets are not redirected and are forwarded by using the standard routing tables.
- The number of available policy-based routing (PBR) labels are reduced as more interfaces are enabled for WCCP ingress redirection. For every interface that supports service groups, one label is consumed. The WCCP labels are taken from the PBR labels. You need to monitor and manage the labels that are available between PBR and WCCP. When labels are not available, the switch cannot add service groups. However, if another interface has the same sequence of service groups, a new label is not needed, and the group can be added to the interface.
- The routing maximum transmission unit (MTU) size configured on the stack member switches should be larger than the client MTU size. The MAC-layer MTU size configured on ports connected to application engines should take into account the GRE tunnel header bytes.
- You cannot configure WCCP and VPN routing/forwarding (VRF) on the same switch interface.
Enabling the Cache Service

For WCCP packet redirection to operate, you must configure the switch interface connected to the client to redirect inbound packets.

This procedure shows how to configure these features on routed ports. To configure these features on SVIs, see the configuration examples that follow the procedure.

Before configuring WCCP commands, configure the SDM template, and reboot the switch. For more information, see Chapter 7, “Configuring SDM Templates.”

Beginning in privileged EXEC mode, follow these steps to enable the cache service, to set a multicast group address or group list, to configure routed interfaces, to redirect inbound packets received from a client to the application engine, enable an interface to listen for a multicast address, and to set a password. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**ip wccp [web-cache</td>
</tr>
<tr>
<td></td>
<td>Enable the cache service, and specify the service number which corresponds to a dynamic service that is defined by the application engine. By default, this feature is disabled.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For <strong>group-address groupaddress</strong>, specify the multicast group address used by the switches and the application engines to participate in the service group.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For <strong>group-list access-list</strong>, if a multicast group address is not used, specify a list of valid IP addresses that correspond to the application engines that are participating in the service group.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For <strong>redirect-list access-list</strong>, specify the redirect service for specific hosts or specific packets from hosts.</td>
</tr>
<tr>
<td></td>
<td>(Optional) For <strong>password encryption-number password</strong>, specify an encryption number. The range is 0 to 7. Use 0 for not encrypted, and use 7 for proprietary. Specify a password name up to seven characters in length. The switch combines the password with the MD5 authentication value to create security for the connection between the switch and the application engine. By default, no password is configured, and no authentication is performed.</td>
</tr>
<tr>
<td></td>
<td>You must configure the same password on each application engine.</td>
</tr>
<tr>
<td></td>
<td>When authentication is enabled, the switch discards messages that are not authenticated.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the interface connected to the application engine or the server, and enter interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>no switchport</strong></td>
</tr>
<tr>
<td></td>
<td>Enter Layer 3 mode.</td>
</tr>
</tbody>
</table>
### Configuring Cache Services By Using WCCP

#### Chapter 44

**Configuring WCCP**

**To disable the cache service, use the** `no ip wccp web-cache` **global configuration command. To disable inbound packet redirection, use the** `no ip wccp web-cache redirect in` **interface configuration command.**

After completing this procedure, configure the application engines in the network.

This example shows how to configure routed interfaces and to enable the cache service with a multicast group address and a redirect access list. Gigabit Ethernet port 1 is connected to the application engine, is configured as a routed port with an IP address of 172.20.10.30, and is re-enabled. Gigabit Ethernet port 2 is connected through the Internet to the server, is configured as a routed port with an IP address of 175.20.20.10, and is re-enabled. Gigabit Ethernet ports 3 to 6 are connected to the clients and are configured as routed ports with IP addresses 175.20.30.20, 175.20.40.30, 175.20.50.40, and 175.20.60.50. The switch listens for multicast traffic and redirects packets received from the client interfaces to the application engine.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td><code>ip address ip-address subnet-mask</code> Configure the IP address and subnet mask.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>no shutdown</code> Enable the interface.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>exit</code> Return to global configuration mode. Repeat Steps 3 through 7 for each application engine and server.</td>
</tr>
<tr>
<td>Step 8</td>
<td><code>interface interface-id</code> Specify the interface connected to the client, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 9</td>
<td><code>no switchport</code> Enter Layer 3 mode.</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>ip address ip-address subnet-mask</code> Configure the IP address and subnet mask.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>no shutdown</code> Enable the interface.</td>
</tr>
<tr>
<td>Step 12</td>
<td>`ip wccp [web-cache</td>
</tr>
<tr>
<td>Step 13</td>
<td>`ip wccp [web-cache</td>
</tr>
<tr>
<td>Step 14</td>
<td><code>exit</code> Return to global configuration mode. Repeat Steps 8 through 13 for each client.</td>
</tr>
<tr>
<td>Step 15</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 16</td>
<td><code>show ip wccp web-cache</code> and <code>show running-config</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 17</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable the cache service, use the `no ip wccp web-cache` global configuration command. To disable inbound packet redirection, use the `no ip wccp web-cache redirect in` interface configuration command. After completing this procedure, configure the application engines in the network.

Switch# configure terminal
Switch(config)# ip wccp web-cache 80 group-address 224.1.1.100 redirect list 12
Switch(config)# access-list 12 permit host 10.1.1.1
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

---

**OL-8553-08**

**Catalyst 3560 Switch Software Configuration Guide**

44-7
This example shows how to configure SVIs and how to enable the cache service with a multicast group list. VLAN 299 is created and configured with an IP address of 175.20.20.10. Gigabit Ethernet port 1 is connected through the Internet to the server and is configured as an access port in VLAN 299. VLAN 300 is created and configured with an IP address of 172.20.10.30. Gigabit Ethernet port 2 is connected to the application engine and is configured as an access port in VLAN 300. VLAN 301 is created and configured with an IP address of 175.20.30.50. Fast Ethernet ports 3 to 6, which are connected to the clients, are configured as access ports in VLAN 301. The switch redirects packets received from the client interfaces to the application engine.

Only permit ACL entries are being used in the redirect-list; deny entries are unsupported.
### Monitoring and Maintaining WCCP

To monitor and maintain WCCP, use one or more of the privileged EXEC commands in Table 44-2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip wccp web-cache</td>
<td>Removes statistics for the web-cache service.</td>
</tr>
<tr>
<td>show ip wccp web-cache</td>
<td>Displays global information related to WCCP.</td>
</tr>
<tr>
<td>show ip wccp web-cache detail</td>
<td>Displays information for the switch and all application engines in the WCCP cluster.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays status about any IP WCCP redirection commands that are configured on an interface; for example, Web Cache Redirect is enabled / disabled.</td>
</tr>
<tr>
<td>show ip wccp web-cache view</td>
<td>Displays which other members have or have not been detected.</td>
</tr>
</tbody>
</table>
Configuring IP Multicast Routing

This chapter describes how to configure IP multicast routing on the Catalyst 3560 switch. IP multicasting is a more efficient way to use network resources, especially for bandwidth-intensive services such as audio and video. IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packet, and IP multicast routers and multilayer switches forward incoming IP multicast packets out all interfaces that lead to members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

To use the IP multicast routing features, the switch must be running the IP services image. To use the PIM stub routing feature, the switch can be running the IP base image.

For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Understanding Cisco’s Implementation of IP Multicast Routing, page 45-1
- Configuring IP Multicast Routing, page 45-10
- Configuring Advanced PIM Features, page 45-35
- Configuring Optional IGMP Features, page 45-38
- Configuring Optional Multicast Routing Features, page 45-44
- Configuring Basic DVMRP Interoperability Features, page 45-48
- Configuring Advanced DVMRP Interoperability Features, page 45-53
- Monitoring and Maintaining IP Multicast Routing, page 45-61

For information on configuring the Multicast Source Discovery Protocol (MSDP), see Chapter 46, “Configuring MSDP.”

Understanding Cisco’s Implementation of IP Multicast Routing

The Cisco IOS software supports these protocols to implement IP multicast routing:

- Internet Group Management Protocol (IGMP) is used among hosts on a LAN and the routers (and multilayer switches) on that LAN to track the multicast groups of which hosts are members.
• Protocol-Independent Multicast (PIM) protocol is used among routers and multilayer switches to track which multicast packets to forward to each other and to their directly connected LANs.

• Distance Vector Multicast Routing Protocol (DVMRP) is used on the multicast backbone of the Internet (MBONE). The software supports PIM-to-DVMRP interaction.

• Cisco Group Management Protocol (CGMP) is used on Cisco routers and multilayer switches connected to Layer 2 Catalyst switches to perform tasks similar to those performed by IGMP.

Figure 45-1 shows where these protocols operate within the IP multicast environment.

**Figure 45-1  IP Multicast Routing Protocols**

According to IPv4 multicast standards, the MAC destination multicast address begins with 0100:5e and is appended by the last 23 bits of the IP address. On the Catalyst 3560 switch, if the multicast packet does not match the switch multicast address, the packets are treated in this way:

• If the packet has a multicast IP address and a unicast MAC address, the packet is forwarded in software. This can occur because some protocols on legacy devices use unicast MAC addresses with multicast IP addresses.

• If the packet has a multicast IP address and an unmatched multicast MAC address, the packet is dropped.

This section has information about these topics:

- Understanding IGMP, page 45-2
- Understanding PIM, page 45-3
- Understanding DVMRP, page 45-9
- Understanding CGMP, page 45-9

### Understanding IGMP

To participate in IP multicasting, multicast hosts, routers, and multilayer switches must have the IGMP operating. This protocol defines the querier and host roles:

• A querier is a network device that sends query messages to discover which network devices are members of a given multicast group.
Chapter 45 Configuring IP Multicast Routing

Understanding Cisco’s Implementation of IP Multicast Routing

- A host is a receiver that sends report messages (in response to query messages) to inform a querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts use IGMP messages to join and leave multicast groups.

Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time. How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it can be very short-lived. Membership in a group can constantly change. A group that has members can have no activity.

IP multicast traffic uses group addresses, which are class D addresses. The high-order bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 through 239.255.255.255. Multicast addresses in the range 224.0.0.0 to 224.0.0.255 are reserved for use by routing protocols and other network control traffic. The address 224.0.0.0 is guaranteed not to be assigned to any group.

IGMP packets are sent using these IP multicast group addresses:
- IGMP general queries are destined to the address 224.0.0.1 (all systems on a subnet).
- IGMP group-specific queries are destined to the group IP address for which the switch is querying.
- IGMP group membership reports are destined to the group IP address for which the switch is reporting.
- IGMP Version 2 (IGMPv2) leave messages are destined to the address 224.0.0.2 (all-multicast-routers on a subnet). In some old host IP stacks, leave messages might be destined to the group IP address rather than to the all-routers address.

**IGMP Version 1**

IGMP Version 1 (IGMPv1) primarily uses a query-response model that enables the multicast router and multilayer switch to find which multicast groups are active (have one or more hosts interested in a multicast group) on the local subnet. IGMPv1 has other processes that enable a host to join and leave a multicast group. For more information, see RFC 1112.

**IGMP Version 2**

IGMPv2 extends IGMP functionality by providing such features as the IGMP leave process to reduce leave latency, group-specific queries, and an explicit maximum query response time. IGMPv2 also adds the capability for routers to elect the IGMP querier without depending on the multicast protocol to perform this task. For more information, see RFC 2236.

**Understanding PIM**

PIM is called *protocol-independent*: regardless of the unicast routing protocols used to populate the unicast routing table, PIM uses this information to perform multicast forwarding instead of maintaining a separate multicast routing table.

PIM is defined in RFC 2362, *Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*. PIM is defined in these Internet Engineering Task Force (IETF) Internet drafts:
Understanding Cisco's Implementation of IP Multicast Routing

**Protocol Independent Multicast (PIM): Motivation and Architecture**

**Protocol Independent Multicast (PIM), Dense Mode Protocol Specification**

**Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification**

draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2

draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode

### PIM Versions

PIMv2 includes these improvements over PIMv1:

- A single, active rendezvous point (RP) exists per multicast group, with multiple backup RPs. This single RP compares to multiple active RPs for the same group in PIMv1.
- A bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism that enables routers and multilayer switches to dynamically learn the group-to-RP mappings.
- Sparse mode and dense mode are properties of a group, as opposed to an interface. We strongly recommend sparse-dense mode, as opposed to either sparse mode or dense mode only.
- PIM join and prune messages have more flexible encoding for multiple address families.
- A more flexible hello packet format replaces the query packet to encode current and future capability options.
- Register messages to an RP specify whether they are sent by a border router or a designated router.
- PIM packets are no longer inside IGMP packets; they are standalone packets.

### PIM Modes

PIM can operate in dense mode (DM), sparse mode (SM), or in sparse-dense mode (PIM DM-SM), which handles both sparse groups and dense groups at the same time.

#### PIM DM

PIM DM builds source-based multicast distribution trees. In dense mode, a PIM DM router or multilayer switch assumes that all other routers or multilayer switches forward multicast packets for a group. If a PIM DM device receives a multicast packet and has no directly connected members or PIM neighbors present, a prune message is sent back to the source to stop unwanted multicast traffic. Subsequent multicast packets are not flooded to this router or switch on this pruned branch because branches without receivers are pruned from the distribution tree, leaving only branches that contain receivers.

When a new receiver on a previously pruned branch of the tree joins a multicast group, the PIM DM device detects the new receiver and immediately sends a graft message up the distribution tree toward the source. When the upstream PIM DM device receives the graft message, it immediately puts the interface on which the graft was received into the forwarding state so that the multicast traffic begins flowing to the receiver.

#### PIM SM

PIM SM uses shared trees and shortest-path-trees (SPTs) to distribute multicast traffic to multicast receivers in the network. In PIM SM, a router or multilayer switch assumes that other routers or switches do not forward multicast packets for a group, unless there is an explicit request for the traffic (join
message). When a host joins a multicast group using IGMP, its directly connected PIM SM device sends PIM join messages toward the root, also known as the RP. This join message travels router-by-router toward the root, constructing a branch of the shared tree as it goes.

The RP keeps track of multicast receivers. It also registers sources through register messages received from the source’s first-hop router (designated router [DR]) to complete the shared tree path from the source to the receiver. When using a shared tree, sources must send their traffic to the RP so that the traffic reaches all receivers.

Prune messages are sent up the distribution tree to prune multicast group traffic. This action permits branches of the shared tree or SPT that were created with explicit join messages to be torn down when they are no longer needed.

### PIM Stub Routing

The PIM stub routing feature, available in all software images, reduces resource usage by moving routed traffic closer to the end user.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP base image contains only PIM stub routing. The IP services image contains complete multicast routing. On a switch running the IP base image, if you try to configure a VLAN interface with PIM dense-mode, sparse-mode, or dense-sparse-mode, the configuration is not allowed.</td>
</tr>
</tbody>
</table>

In a network using PIM stub routing, the only allowable route for IP traffic to the user is through a switch that is configured with PIM stub routing. PIM passive interfaces are connected to Layer 2 access domains, such as VLANs, or to interfaces that are connected to other Layer 2 devices. Only directly connected multicast (IGMP) receivers and sources are allowed in the Layer 2 access domains. The PIM passive interfaces do not send or process any received PIM control packets.

When using PIM stub routing, you should configure the distribution and remote routers to use IP multicast routing and configure only the switch as a PIM stub router. The switch does not route transit traffic between distribution routers. You also need to configure a routed uplink port on the switch. The switch uplink port cannot be used with SVIs. If you need PIM for an SVI uplink port, you should upgrade to the IP services feature set.

You must also configure EIGRP stub routing when configuring PIM stub routing on the switch. For more information, see the “Configuring EIGRP Stub Routing” section on page 37-39.

The redundant PIM stub router topology is not supported. The redundant topology exists when there is more than one PIM router forwarding multicast traffic to a single access domain. PIM messages are blocked, and the PIM asset and designated router election mechanisms are not supported on the PIM passive interfaces. Only the nonredundant access router topology is supported by the PIM stub feature. By using a nonredundant topology, the PIM passive interface assumes that it is the only interface and designated router on that access domain.

The PIM stub feature is enforced in the IP base image. If you upgrade to a higher software version, the PIM stub configuration remains until you reconfigure the interfaces.

In Figure 45-2, Switch A routed uplink port 25 is connected to the router and PIM stub routing is enabled on the VLAN 100 interfaces and on Host 3. This configuration allows the directly connected hosts to receive traffic from multicast source 200.1.1.3. See the “Configuring PIM Stub Routing” section on page 45-22 for more information.
### IGMP Helper

PIM stub routing moves routed traffic closer to the end user and reduces network traffic. You can also reduce traffic by configuring a stub router (switch) with the IGMP helper feature.

You can configure a stub router (switch) with the `igmp helper help-address` interface configuration command to enable the switch to send reports to the next-hop interface. Hosts that are not directly connected to a downstream router can then join a multicast group sourced from an upstream network. The IGMP packets from a host wanting to join a multicast stream are forwarded upstream to the next-hop device when this feature is configured. When the upstream central router receives the helper IGMP reports or leaves, it adds or removes the interfaces from its outgoing interface list for that group.

For complete syntax and usage information for the `ip igmp helper-address` command, see the *Cisco IOS IP and IP Routing Command Reference, Release 12.1*.

### Auto-RP

This proprietary feature eliminates the need to manually configure the RP information in every router and multilayer switch in the network. For auto-RP to work, you configure a Cisco router or multilayer switch as the mapping agent. It uses IP multicast to learn which routers or switches in the network are possible candidate RPs to receive candidate RP announcements. Candidate RPs periodically send multicast RP-announce messages to a particular group or group range to announce their availability.

Mapping agents listen to these candidate RP announcements and use the information to create entries in their Group-to-RP mapping caches. Only one mapping cache entry is created for any Group-to-RP range received, even if multiple candidate RPs are sending RP announcements for the same range. As the RP-announce messages arrive, the mapping agent selects the router or switch with the highest IP address as the active RP and stores this RP address in the Group-to-RP mapping cache.

Mapping agents periodically multicast the contents of their Group-to-RP mapping caches. Thus, all routers and switches automatically discover which RP to use for the groups that they support. If a router or switch fails to receive RP-discovery messages and the Group-to-RP mapping information expires, it changes to a statically configured RP that was defined with the `ip pim rp-address` global configuration command. If no statically configured RP exists, the router or switch changes the group to dense-mode operation.

Multiple RPs serve different group ranges or serve as hot backups of each other.
Bootstrap Router

PIMv2 BSR is another method to distribute group-to-RP mapping information to all PIM routers and multilayer switches in the network. It eliminates the need to manually configure RP information in every router and switch in the network. However, instead of using IP multicast to distribute group-to-RP mapping information, BSR uses hop-by-hop flooding of special BSR messages to distribute the mapping information.

The BSR is elected from a set of candidate routers and switches in the domain that have been configured to function as BSRs. The election mechanism is similar to the root-bridge election mechanism used in bridged LANs. The BSR election is based on the BSR priority of the device contained in the BSR messages that are sent hop-by-hop through the network. Each BSR device examines the message and forwards out all interfaces only the message that has either a higher BSR priority than its BSR priority or the same BSR priority, but with a higher BSR IP address. Using this method, the BSR is elected.

The elected BSR sends BSR messages with a TTL of 1. Neighboring PIMv2 routers or multilayer switches receive the BSR message and multicast it out all other interfaces (except the one on which it was received) with a TTL of 1. In this way, BSR messages travel hop-by-hop throughout the PIM domain. Because BSR messages contain the IP address of the current BSR, the flooding mechanism enables candidate RPs to automatically learn which device is the elected BSR.

Candidate RPs send candidate RP advertisements showing the group range for which they are responsible to the BSR, which stores this information in its local candidate-RP cache. The BSR periodically advertises the contents of this cache in BSR messages to all other PIM devices in the domain. These messages travel hop-by-hop through the network to all routers and switches, which store the RP information in the BSR message in their local RP cache. The routers and switches select the same RP for a given group because they all use a common RP hashing algorithm.

Multicast Forwarding and Reverse Path Check

With unicast routing, routers and multilayer switches forward traffic through the network along a single path from the source to the destination host whose IP address appears in the destination address field of the IP packet. Each router and switch along the way makes a unicast forwarding decision, using the destination IP address in the packet, by looking up the destination address in the unicast routing table and forwarding the packet through the specified interface to the next hop toward the destination.
With multicasting, the source is sending traffic to an arbitrary group of hosts represented by a multicast group address in the destination address field of the IP packet. To decide whether to forward or drop an incoming multicast packet, the router or multilayer switch uses a reverse path forwarding (RPF) check on the packet as follows and shown in Figure 45-3:

1. The router or multilayer switch examines the source address of the arriving multicast packet to decide whether the packet arrived on an interface that is on the reverse path back to the source.

2. If the packet arrives on the interface leading back to the source, the RPF check is successful and the packet is forwarded to all interfaces in the outgoing interface list (which might not be all interfaces on the router).

3. If the RPF check fails, the packet is discarded.

Some multicast routing protocols, such as DVMRP, maintain a separate multicast routing table and use it for the RPF check. However, PIM uses the unicast routing table to perform the RPF check.

Figure 45-3 shows port 2 receiving a multicast packet from source 151.10.3.21. Table 45-1 shows that the port on the reverse path to the source is port 1, not port 2. Because the RPF check fails, the multilayer switch discards the packet. Another multicast packet from source 151.10.3.21 is received on port 1, and the routing table shows this port is on the reverse path to the source. Because the RPF check passes, the switch forwards the packet to all port in the outgoing port list.

PIM uses both source trees and RP-rooted shared trees to forward datagrams (described in the “PIM DM” section on page 45-4 and the “PIM SM” section on page 45-4). The RPF check is performed differently for each:

- If a PIM router or multilayer switch has a source-tree state (that is, an (S,G) entry is present in the multicast routing table), it performs the RPF check against the IP address of the source of the multicast packet.
- If a PIM router or multilayer switch has a shared-tree state (and no explicit source-tree state), it performs the RPF check on the RP address (which is known when members join the group).
Sparse-mode PIM uses the RPF lookup function to decide where it needs to send joins and prunes:

- (S,G) joins (which are source-tree states) are sent toward the source.
- (*,G) joins (which are shared-tree states) are sent toward the RP.

DVMRP and dense-mode PIM use only source trees and use RPF as previously described.

Understanding DVMRP

DVMRP is implemented in the equipment of many vendors and is based on the public-domain mrouted program. This protocol has been deployed in the MBONE and in other intradomain multicast networks.

Cisco routers and multilayer switches run PIM and can forward multicast packets to and receive from a DVMRP neighbor. It is also possible to propagate DVMRP routes into and through a PIM cloud. The software propagates DVMRP routes and builds a separate database for these routes on each router and multilayer switch, but PIM uses this routing information to make the packet-forwarding decision. The software does not implement the complete DVMRP. However, it supports dynamic discovery of DVMRP routers and can interoperate with them over traditional media (such as Ethernet and FDDI) or over DVMRP-specific tunnels.

DVMRP neighbors build a route table by periodically exchanging source network routing information in route-report messages. The routing information stored in the DVMRP routing table is separate from the unicast routing table and is used to build a source distribution tree and to perform multicast forward using RPF.

DVMRP is a dense-mode protocol and builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths. Forwarding occurs until prune messages are received on those parent-child links, which further constrain the broadcast of multicast packets.

Understanding CGMP

This software release provides CGMP-server support on your switch; no client-side functionality is provided. The switch serves as a CGMP server for devices that do not support IGMP snooping but have CGMP-client functionality.

CGMP is a protocol used on Cisco routers and multilayer switches connected to Layer 2 Catalyst switches to perform tasks similar to those performed by IGMP. CGMP permits Layer 2 group membership information to be communicated from the CGMP server to the switch. The switch can then learn on which interfaces multicast members reside instead of flooding multicast traffic to all switch interfaces. (IGMP snooping is another method to constrain the flooding of multicast packets. For more information, see Chapter 22, “Configuring IGMP Snooping and MVR.”)

CGMP is necessary because the Layer 2 switch cannot distinguish between IP multicast data packets and IGMP report messages, which are both at the MAC-level and are addressed to the same group address.

CGMP is mutually exclusive with HSRPv1. You cannot enable CGMP leaving processing and HSRPv1 at the same time. However, you can enable CGMP and HSRPv2 at the same time. For more information, see the “HSRP Versions” section on page 41-3.
Configuring IP Multicast Routing

These sections contain this configuration information:

- Default Multicast Routing Configuration, page 45-10
- Multicast Routing Configuration Guidelines, page 45-10
- Configuring Basic Multicast Routing, page 45-12 (required)
- Configuring Source-Specific Multicast, page 45-13
- Configuring Source Specific Multicast Mapping, page 45-17
- Configuring PIM Stub Routing, page 45-22 (optional)
- Configuring a Rendezvous Point, page 45-24 (required if the interface is in sparse-dense mode, and you want to treat the group as a sparse group)
- Using Auto-RP and a BSR, page 45-34 (required for non-Cisco PIMv2 devices to interoperate with Cisco PIM v1 devices)
- Monitoring the RP Mapping Information, page 45-34 (optional)
- Troubleshooting PIMv1 and PIMv2 Interoperability Problems, page 45-35 (optional)

Default Multicast Routing Configuration

Table 45-2 shows the default multicast routing configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing</td>
<td>Disabled on all interfaces.</td>
</tr>
<tr>
<td>PIM version</td>
<td>Version 2.</td>
</tr>
<tr>
<td>PIM mode</td>
<td>No mode is defined.</td>
</tr>
<tr>
<td>PIM stub routing</td>
<td>None configured.</td>
</tr>
<tr>
<td>PIM RP address</td>
<td>None configured.</td>
</tr>
<tr>
<td>PIM domain border</td>
<td>Disabled.</td>
</tr>
<tr>
<td>PIM multicast boundary</td>
<td>None.</td>
</tr>
<tr>
<td>Candidate BSRs</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Candidate RPs</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Shortest-path tree threshold rate</td>
<td>0 kb/s.</td>
</tr>
<tr>
<td>PIM router query message interval</td>
<td>30 seconds.</td>
</tr>
</tbody>
</table>

Multicast Routing Configuration Guidelines

To avoid misconfiguring multicast routing on your switch, review the information in these sections:

- PIMv1 and PIMv2 Interoperability, page 45-11
- Auto-RP and BSR Configuration Guidelines, page 45-11
PIMv1 and PIMv2 Interoperability

The Cisco PIMv2 implementation provides interoperability and transition between Version 1 and Version 2, although there might be some minor problems.

You can upgrade to PIMv2 incrementally. PIM Versions 1 and 2 can be configured on different routers and multilayer switches within one network. Internally, all routers and multilayer switches on a shared media network must run the same PIM version. Therefore, if a PIMv2 device detects a PIMv1 device, the Version 2 device downgrades itself to Version 1 until all Version 1 devices have been shut down or upgraded.

PIMv2 uses the BSR to discover and announce RP-set information for each group prefix to all the routers and multilayer switches in a PIM domain. PIMv1, together with the Auto-RP feature, can perform the same tasks as the PIMv2 BSR. However, Auto-RP is a standalone protocol, separate from PIMv1, and is a proprietary Cisco protocol. PIMv2 is a standards track protocol in the IETF. We recommend that you use PIMv2. The BSR mechanism interoperates with Auto-RP on Cisco routers and multilayer switches. For more information, see the “Auto-RP and BSR Configuration Guidelines” section on page 45-11.

When PIMv2 devices interoperate with PIMv1 devices, Auto-RP should have already been deployed. A PIMv2 BSR that is also an Auto-RP mapping agent automatically advertises the RP elected by Auto-RP. That is, Auto-RP sets its single RP on every router or multilayer switch in the group. Not all routers and switches in the domain use the PIMv2 hash function to select multiple RPs.

Dense-mode groups in a mixed PIMv1 and PIMv2 region need no special configuration; they automatically interoperate.

Sparse-mode groups in a mixed PIMv1 and PIMv2 region are possible because the Auto-RP feature in PIMv1 interoperates with the PIMv2 RP feature. Although all PIMv2 devices can also use PIMv1, we recommend that the RPs be upgraded to PIMv2. To ease the transition to PIMv2, we have these recommendations:

- Use Auto-RP throughout the region.
- Configure sparse-dense mode throughout the region.

If Auto-RP is not already configured in the PIMv1 regions, configure Auto-RP. For more information, see the “Configuring Auto-RP” section on page 45-26.

Auto-RP and BSR Configuration Guidelines

There are two approaches to using PIMv2. You can use Version 2 exclusively in your network or migrate to Version 2 by employing a mixed PIM version environment.

- If your network is all Cisco routers and multilayer switches, you can use either Auto-RP or BSR.
- If you have non-Cisco routers in your network, you must use BSR.
- If you have Cisco PIMv1 and PIMv2 routers and multilayer switches and non-Cisco routers, you must use both Auto-RP and BSR. If your network includes routers from other vendors, configure the Auto-RP mapping agent and the BSR on a Cisco PIMv2 device. Ensure that no PIMv1 device is located in the path a between the BSR and a non-Cisco PIMv2 device.
- Because bootstrap messages are sent hop-by-hop, a PIMv1 device prevents these messages from reaching all routers and multilayer switches in your network. Therefore, if your network has a PIMv1 device in it and only Cisco routers and multilayer switches, it is best to use Auto-RP.
• If you have a network that includes non-Cisco routers, configure the Auto-RP mapping agent and the BSR on a Cisco PIMv2 router or multilayer switch. Ensure that no PIMv1 device is on the path between the BSR and a non-Cisco PIMv2 router.

• If you have non-Cisco PIMv2 routers that need to interoperate with Cisco PIMv1 routers and multilayer switches, both Auto-RP and a BSR are required. We recommend that a Cisco PIMv2 device be both the Auto-RP mapping agent and the BSR. For more information, see the “Using Auto-RP and a BSR” section on page 45-34.

Configuring Basic Multicast Routing

You must enable IP multicast routing and configure the PIM version and the PIM mode. Then the software can forward multicast packets, and the switch can populate its multicast routing table.

You can configure an interface to be in PIM dense mode, sparse mode, or sparse-dense mode. The switch populates its multicast routing table and forwards multicast packets it receives from its directly connected LANs according to the mode setting. You must enable PIM in one of these modes for an interface to perform IP multicast routing. Enabling PIM on an interface also enables IGMP operation on that interface.

Note

If you enable PIM on multiple interfaces, when most of them are not on the outgoing interface list, and IGMP snooping is disabled, the outgoing interface might not be able to sustain line rate for multicast traffic because of the extra replication.

In populating the multicast routing table, dense-mode interfaces are always added to the table. Sparse-mode interfaces are added to the table only when periodic join messages are received from downstream devices or when there is a directly connected member on the interface. When forwarding from a LAN, sparse-mode operation occurs if there is an RP known for the group. If so, the packets are encapsulated and sent toward the RP. When no RP is known, the packet is flooded in a dense-mode fashion. If the multicast traffic from a specific source is sufficient, the receiver’s first-hop router might send join messages toward the source to build a source-based distribution tree.

By default, multicast routing is disabled, and there is no default mode setting. This procedure is required.

Beginning in privileged EXEC mode, follow these steps to enable IP multicasting, to configure a PIM version, and to configure a PIM mode. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip multicast-routing distributed Enable IP multicast distributed switching.</td>
</tr>
</tbody>
</table>
Configuring IP Multicast Routing

To disable multicasting, use the **no ip multicast-routing distributed** global configuration command. To return to the default PIM version, use the **no ip pim version** interface configuration command. To disable PIM on an interface, use the **no ip pim** interface configuration command.

### Configuring Source-Specific Multicast

This section describes how to configure source-specific multicast (SSM). For a complete description of the SSM commands in this section, refer to the “IP Multicast Routing Commands” chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*. To locate documentation for other commands that appear in this chapter, use the command reference master index, or search online.
The SSM feature is an extension of IP multicast in which datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only SSM distribution trees (no shared trees) are created.

SSM Components Overview

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments. The switch supports these components that support the implementation of SSM:

- Protocol independent multicast source-specific mode (PIM-SSM)
  PIM-SSM is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM).
- Internet Group Management Protocol version 3 (IGMPv3)
  To run SSM with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The current IP multicast infrastructure in the Internet and many enterprise intranets is based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have the limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic.

The ISM service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems receive this traffic by becoming members of the host group.

Membership in a host group simply requires signalling the host group through IGMP version 1, 2, or 3. In SSM, delivery of datagrams is based on (S, G) channels. In both SSM and ISM, no signalling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signalling use IGMP include mode membership reports, which are supported only in IGMP version 3.

SSM IP Address Range

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. Cisco IOS software allows SSM configuration for the IP multicast address range of 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use an address in the SSM range (unless the application is modified to use an explicit (S, G) channel subscription).
SSM Operations

An established network, in which IP multicast service is based on PIM-SM, can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM (for example, MSDP, Auto-RP, or bootstrap router [BSR]) if only SSM service is needed.

If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers support SSM. Routers that are not directly connected to receivers do not require support for SSM. In general, these not-last-hop routers must only run PIM-SM in the SSM range and might need additional access control configuration to suppress MSDP signalling, registering, or PIM-SM shared tree operations from occurring within the SSM range.

Use the `ip pim ssm` global configuration command to configure the SSM range and to enable SSM. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 include-mode membership reports.
- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-SM. In this mode, only PIM (S, G) join and prune messages are generated by the router, and no (S, G) rendezvous point tree (RPT) or (*, G) RPT messages are generated. Incoming messages related to RPT operations are ignored or rejected, and incoming PIM register messages are immediately answered with register-stop messages. PIM-SSM is backward-compatible with PIM-SM unless a router is a last-hop router. Therefore, routers that are not last-hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- No MSDP source-active (SA) messages within the SSM range are accepted, generated, or forwarded.

IGMPv3 Host Signalling

In IGMPv3, hosts signal membership to last hop routers of multicast groups. Hosts can signal group membership with filtering capabilities with respect to sources. A host can either signal that it wants to receive traffic from all sources sending to a group except for some specific sources (called exclude mode), or that it wants to receive traffic only from some specific sources sending to the group (called include mode).

IGMPv3 can operate with both ISM and SSM. In ISM, both exclude and include mode reports are applicable. In SSM, only include mode reports are accepted by the last-hop router. Exclude mode reports are ignored.

Configuration Guidelines

This section contains the guidelines for configuring SSM.

Legacy Applications Within the SSM Range Restrictions

Existing applications in a network predating SSM do not work within the SSM range unless they are modified to support (S, G) channel subscriptions. Therefore, enabling SSM in a network can cause problems for existing applications if they use addresses within the designated SSM range.
Address Management Restrictions

Address management is still necessary to some degree when SSM is used with Layer 2 switching mechanisms. Cisco Group Management Protocol (CGMP), IGMP snooping, or Router-Port Group Management Protocol (RGMP) support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, they do not benefit from these existing mechanisms. Instead, both receivers receive all (S, G) channel traffic and filter out the unwanted traffic on input. Because SSM can re-use the group addresses in the SSM range for many independent applications, this situation can lead to decreased traffic filtering in a switched network. For this reason, it is important to use random IP addresses from the SSM range for an application to minimize the chance for re-use of a single address within the SSM range between different applications. For example, an application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup guarantees that multiple receivers to different channels within the same application service never experience traffic aliasing in networks that include Layer 2 switches.

IGMP Snooping and CGMP Limitations

IGMPv3 uses new membership report messages that might not be correctly recognized by older IGMP snooping switches.

For more information about switching issues related to IGMP (especially with CGMP), see the “Understanding IGMP” section on page 45-2.

State Maintenance Limitations

In PIM-SSM, the last hop router continues to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source is maintained, even if the source does not send traffic for longer periods of time (or even never).

This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S, G) state is deleted and only re-established after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

Configuring SSM

Beginning in privileged EXEC mode, follow these steps to configure SSM:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>ip pim ssm [default</td>
<td>Define the SSM range of IP multicast addresses.</td>
</tr>
<tr>
<td>range access-list]</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>interface type number</td>
<td>Select an interface that is connected to hosts on which IGMPv3</td>
</tr>
<tr>
<td></td>
<td>can be enabled, and enter the interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>ip pim [sparse-mode</td>
<td>Enable PIM on an interface. You must use either sparse mode</td>
</tr>
<tr>
<td>sparse-dense-mode]</td>
<td>or sparse-dense mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>ip igmp version 3</td>
<td>Enable IGMPv3 on this interface. The default version of IGMP is set to</td>
</tr>
<tr>
<td></td>
<td>Version 2.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Configuring IP Multicast Routing

Chapter 45      Configuring IP Multicast Routing

Address Management Restrictions

Address management is still necessary to some degree when SSM is used with Layer 2 switching mechanisms. Cisco Group Management Protocol (CGMP), IGMP snooping, or Router-Port Group Management Protocol (RGMP) support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, they do not benefit from these existing mechanisms. Instead, both receivers receive all (S, G) channel traffic and filter out the unwanted traffic on input. Because SSM can re-use the group addresses in the SSM range for many independent applications, this situation can lead to decreased traffic filtering in a switched network. For this reason, it is important to use random IP addresses from the SSM range for an application to minimize the chance for re-use of a single address within the SSM range between different applications. For example, an application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup guarantees that multiple receivers to different channels within the same application service never experience traffic aliasing in networks that include Layer 2 switches.

IGMP Snooping and CGMP Limitations

IGMPv3 uses new membership report messages that might not be correctly recognized by older IGMP snooping switches.

For more information about switching issues related to IGMP (especially with CGMP), see the “Understanding IGMP” section on page 45-2.

State Maintenance Limitations

In PIM-SSM, the last hop router continues to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source is maintained, even if the source does not send traffic for longer periods of time (or even never).

This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S, G) state is deleted and only re-established after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

Configuring SSM

Beginning in privileged EXEC mode, follow these steps to configure SSM:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>ip pim ssm [default</td>
<td>Define the SSM range of IP multicast addresses.</td>
</tr>
<tr>
<td>range access-list]</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td></td>
</tr>
<tr>
<td>interface type number</td>
<td>Select an interface that is connected to hosts on which IGMPv3</td>
</tr>
<tr>
<td></td>
<td>can be enabled, and enter the interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td></td>
</tr>
<tr>
<td>ip pim [sparse-mode</td>
<td>Enable PIM on an interface. You must use either sparse mode</td>
</tr>
<tr>
<td>sparse-dense-mode]</td>
<td>or sparse-dense mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>ip igmp version 3</td>
<td>Enable IGMPv3 on this interface. The default version of IGMP is set to</td>
</tr>
<tr>
<td></td>
<td>Version 2.</td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to monitor SSM.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp groups detail</td>
<td>Display the (S, G) channel subscription through IGMPv3.</td>
</tr>
<tr>
<td>show ip mroute</td>
<td>Display whether a multicast group supports SSM service or whether a source-specific host report was received.</td>
</tr>
</tbody>
</table>

Configuring Source Specific Multicast Mapping

The Source Specific Multicast (SSM) mapping feature supports SSM transition when supporting SSM on the end system is impossible or unwanted due to administrative or technical reasons. You can use SSM mapping to leverage SSM for video delivery to legacy STBs that do not support IGMPv3 or for applications that do not use the IGMPv3 host stack.

This section covers these topics:

- Configuration Guidelines, page 45-17
- SSM Mapping Overview, page 45-18
- Configuring SSM Mapping, page 45-19
- Monitoring SSM Mapping, page 45-22

Configuration Guidelines

These are the SSM mapping configuration guidelines:

- Before you configure SSM mapping, enable IP multicast routing, enable PIM sparse mode, and configure SSM. For information on enabling IP multicast routing and PIM sparse mode, see the “Default Multicast Routing Configuration” section on page 45-10.

- Before you configure static SSM mapping, you must configure access control lists (ACLs) that define the group ranges to be mapped to source addresses. For information on configuring an ACL, see Chapter 33, “Configuring Network Security with ACLs.”

- Before you can configure and use SSM mapping with DNS lookups, you must be able to add records to a running DNS server. If you do not already have a DNS server running, you need to install one. You can use a product such as Cisco Network Registrar. Go to this URL for more information: http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps5698/ps1982/ps6089/prod_bulletin0900aecd803fc803.html
These are the SSM mapping restrictions:

- The SSM mapping feature does not have all the benefits of full SSM. Because SSM mapping takes a group join from a host and identifies this group with an application associated with one or more sources, it can only support one such application per group. Full SSM applications can still share the same group as in SSM mapping.

- Enable IGMPv3 with care on the last hop router when you rely solely on SSM mapping as a transition solution for full SSM. When you enable both SSM mapping and IGMPv3 and the hosts already support IGMPv3 (but not SSM), the hosts send IGMPv3 group reports. SSM mapping does not support these IGMPv3 group reports, and the router does not correctly associate sources with these reports.

**SSM Mapping Overview**

In a typical STB deployment, each TV channel uses one separate IP multicast group and has one active server host sending the TV channel. A single server can send multiple TV channels, but each to a different group. In this network environment, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group, the report addresses the well-known TV server for the TV channel associated with the multicast group.

When SSM mapping is configured, if a router receives an IGMPv1 or IGMPv2 membership report for a particular group, the router translates this report into one or more channel memberships for the well-known sources associated with this group.

When the router receives an IGMPv1 or IGMPv2 membership report for a group, the router uses SSM mapping to determine one or more source IP addresses for the group. SSM mapping then translates the membership report as an IGMPv3 report and continues as if it had received an IGMPv3 report. The router then sends PIM joins and continues to be joined to these groups as long as it continues to receive the IGMPv1 or IGMPv2 membership reports, and the SSM mapping for the group remains the same.

SSM mapping enables the last hop router to determine the source addresses either by a statically configured table on the router or through a DNS server. When the statically configured table or the DNS mapping changes, the router leaves the current sources associated with the joined groups.

For information on SSM mapping:

**Static SSM Mapping**

With static SSM mapping, you can configure the last hop router to use a static map to determine the sources that are sending to groups. Static SSM mapping requires that you configure ACLs to define group ranges. Then you can map the groups permitted by those ACLs to sources by using the `ip igmp static ssm-map` global configuration command.

You can configure static SSM mapping in smaller networks when a DNS is not needed or to locally override DNS mappings. When configured, static SSM mappings take precedence over DNS mappings.

**DNS-Based SSM Mapping**

You can use DNS-based SSM mapping to configure the last hop router to perform a reverse DNS lookup to determine sources sending to groups. When DNS-based SSM mapping is configured, the router constructs a domain name that includes the group address and performs a reverse lookup into the DNS. The router looks up IP address resource records and uses them as the source addresses associated with this group. SSM mapping supports up to 20 sources for each group. The router joins all sources configured for a group (see Figure 45-4).
The SSM mapping mechanism that enables the last hop router to join multiple sources for a group can provide source redundancy for a TV broadcast. In this context, the last hop router provides redundancy using SSM mapping to simultaneously join two video sources for the same TV channel. However, to prevent the last hop router from duplicating the video traffic, the video sources must use a server-side switchover mechanism. One video source is active, and the other backup video source is passive. The passive source waits until an active source failure is detected before sending the video traffic for the TV channel. Thus, the server-side switchover mechanism ensures that only one of the servers is actively sending video traffic for the TV channel.

To look up one or more source addresses for a group that includes G1, G2, G3, and G4, you must configure these DNS records on the DNS server:

```
   IN A source-address-2
   IN A source-address-n
```

See your DNS server documentation for more information about configuring DNS resource records. For information on SSM mapping:


### Configuring SSM Mapping

- Configuring Static SSM Mapping, page 45-20 (required)
- Configuring DNS-Based SSM Mapping, page 45-20 (required)
- Configuring Static Traffic Forwarding with SSM Mapping, page 45-21 (optional)
Configuring Static SSM Mapping

Beginning in privileged EXEC mode, follow these steps to configure static SSM mapping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp ssm-map enable</td>
</tr>
<tr>
<td>Step 3</td>
<td>no ip igmp ssm-map query dns</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip igmp ssm-map static <em>access-list</em> <em>source-address</em></td>
</tr>
<tr>
<td>Step 5</td>
<td>Repeat Step 4 to configure additional static SSM mappings, if required.</td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

For SSM mapping configuration examples:

Configuring DNS-Based SSM Mapping

To configure DNS-based SSM mapping, you need to create a DNS server zone or add records to an existing zone. If the routers that are using DNS-based SSM mapping are also using DNS for other purposes, you should use a normally configured DNS server. If DNS-based SSM mapping is the only DNS implementation being used on the router, you can configure a false DNS setup with an empty root zone or a root zone that points back to itself.

Beginning in privileged EXEC mode, follow these steps to configure DNS-based SSM mapping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip igmp ssm-map enable</td>
</tr>
</tbody>
</table>
Configuring Static Traffic Forwarding with SSM Mapping

Use static traffic forwarding with SSM mapping to statically forward SSM traffic for certain groups. Beginning in privileged EXEC mode, follow these steps to configure static traffic forwarding with SSM mapping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1   configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2   interface type number     | Select an interface on which to statically forward traffic for a multicast group using SSM mapping, and enter interface configuration mode.  
**Note** Static forwarding of traffic with SSM mapping works with either DNS-based SSM mapping or statically configured SSM mapping.  |
| Step 3   ip igmp static-group group-address source ssm-map | Configure SSM mapping to statically forward a (S, G) channel from the interface. Use this command if you want to statically forward SSM traffic for certain groups. Use DNS-based SSM mapping to determine the source addresses of the channels. |
| Step 4   show running-config       | Verify your entries.                                                     |
| Step 5   copy running-config startup-config | (Optional) Save your entries in the configuration file.                  |
Monitoring SSM Mapping

Use the privileged EXEC commands in Table 45-3 to monitor SSM mapping.

Table 45-3 SSM Mapping Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp ssm-mapping</td>
<td>Display information about SSM mapping.</td>
</tr>
<tr>
<td>show ip igmp ssm-mapping group-address</td>
<td>Display the sources that SSM mapping uses for a particular group.</td>
</tr>
<tr>
<td>show ip igmp groups [group-name</td>
<td>group-address</td>
</tr>
<tr>
<td>show host</td>
<td>Display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.</td>
</tr>
<tr>
<td>debug ip igmp group-address</td>
<td>Display the IGMP packets received and sent and IGMP host-related events.</td>
</tr>
</tbody>
</table>

For SSM mapping monitoring examples:

Configuring PIM Stub Routing

The PIM Stub routing feature supports multicast routing between the distribution layer and the access layer. It supports two types of PIM interfaces, uplink PIM interfaces, and PIM passive interfaces. A routed interface configured with the PIM passive mode does not pass or forward PIM control traffic, it only passes and forwards IGMP traffic.

PIM Stub Routing Configuration Guidelines

Follow these guidelines when enabling PIM stub routing on an interface:

- Before configuring PIM stub routing, you must have IP multicast routing configured on both the stub router and the central router. You must also have PIM mode (dense-mode, sparse-mode, or dense-sparse-mode) configured on the uplink interface of the stub router.
- The PIM stub router does not route the transit traffic between the distribution routers. Unicast (EIGRP) stub routing enforces this behavior. You must configure unicast stub routing to assist the PIM stub router behavior. For more information, see the “Configuring EIGRP Stub Routing” section on page 37-39.
- Only directly connected multicast (IGMP) receivers and sources are allowed in the Layer 2 access domains. The PIM protocol is not supported in access domains.
- The redundant PIM stub router topology is not supported.
Enabling PIM Stub Routing

Beginning in privileged EXEC mode, follow these steps to enable PIM stub routing on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip pim passive</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip pim interface</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable PIM stub routing on an interface, use the **no ip pim passive** interface configuration command.

In this example, IP multicast routing is enabled, Switch A PIM uplink port 25 is configured as a routed uplink port with **spare-dense-mode enabled**. PIM stub routing is enabled on the VLAN 100 interfaces and on Gigabit Ethernet port 20 in Figure 45-2:

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet0/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/20
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
```

To verify that PIM stub is enabled for each interface, use the **show ip pim interface** privileged EXEC command:

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet0/20 v2/P 0 30 1 10.1.1.1
```
Use these privileged EXEC commands to display information about PIM stub configuration and status:

- **show ip pim interface** displays the PIM stub that is enabled on each interface.
- **show ip igmp detail** displays the interested clients that have joined the specific multicast source group.
- **show ip igmp mroute** verifies that the multicast stream forwards from the source to the interested clients.

### Configuring a Rendezvous Point

You must have an RP if the interface is in sparse-dense mode and if you want to treat the group as a sparse group. You can use several methods:

- **Manually Assigning an RP to Multicast Groups, page 45-24**
- **Configuring Auto-RP, page 45-26** (a standalone, Cisco-proprietary protocol separate from PIMv1)
- **Configuring PIMv2 BSR, page 45-30** (a standards track protocol in the Internet Engineering Task Force (IETF))

You can use auto-RP, BSR, or a combination of both, depending on the PIM version that you are running and the types of routers in your network. For more information, see the “PIMv1 and PIMv2 Interoperability” section on page 45-11 and the “Auto-RP and BSR Configuration Guidelines” section on page 45-11.

### Manually Assigning an RP to Multicast Groups

This section explains how to manually configure an RP. If the RP for a group is learned through a dynamic mechanism (such as auto-RP or BSR), you need not perform this task for that RP.

Senders of multicast traffic announce their existence through register messages received from the source first-hop router (designated router) and forwarded to the RP. Receivers of multicast packets use RPs to join a multicast group by using explicit join messages. RPs are not members of the multicast group; rather, they serve as a *meeting place* for multicast sources and group members.

You can configure a single RP for multiple groups defined by an access list. If there is no RP configured for a group, the multilayer switch treats the group as dense and uses the dense-mode PIM techniques.
Beginning in privileged EXEC mode, follow these steps to manually configure the address of the RP. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip pim rp-address ip-address [access-list-number] [override]</td>
</tr>
<tr>
<td></td>
<td>Configure the address of a PIM RP. By default, no PIM RP address is configured. You must configure the IP address of RPs on all routers and multilayer switches (including the RP). If there is no RP configured for a group, the switch treats the group as dense, using the dense-mode PIM techniques. A PIM device can be an RP for more than one group. Only one RP address can be used at a time within a PIM domain. The access-list conditions specify for which groups the device is an RP.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>ip-address</strong>, enter the unicast address of the RP in dotted-decimal notation.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <strong>access-list-number</strong>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) The <strong>override</strong> keyword means that if there is a conflict between the RP configured with this command and one learned by Auto-RP or BSR, the RP configured with this command prevails.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>access-list access-list-number [deny</td>
</tr>
<tr>
<td></td>
<td>Create a standard access list, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>access-list-number</strong>, enter the access list number specified in Step 2.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>deny</strong> keyword denies access if the conditions are matched. The <strong>permit</strong> keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>source</strong>, enter the multicast group address for which the RP should be used.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <strong>source-wildcard</strong>, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove an RP address, use the **no ip pim rp-address ip-address [access-list-number] [override]** global configuration command.

This example shows how to configure the address of the RP to 147.106.6.22 for multicast group 225.2.2.2 only:

Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
Configuring Auto-RP

Auto-RP uses IP multicast to automate the distribution of group-to-RP mappings to all Cisco routers and multilayer switches in a PIM network. It has these benefits:

- It is easy to use multiple RPs within a network to serve different group ranges.
- It provides load splitting among different RPs and arrangement of RPs according to the location of group participants.
- It avoids inconsistent, manual RP configurations on every router and multilayer switch in a PIM network, which can cause connectivity problems.

Follow these guidelines when configuring Auto-RP:

- If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must manually configure an RP as described in the “Manually Assigning an RP to Multicast Groups” section on page 45-24.
- If routed interfaces are configured in sparse mode, Auto-RP can still be used if all devices are configured with a manual RP address for the Auto-RP groups.
- If routed interfaces are configured in sparse mode and you enter the `ip pim autorp listener` global configuration command, Auto-RP can still be used even if all devices are not configured with a manual RP address for the Auto-RP groups.

These sections describe how to configure Auto-RP:

- Setting up Auto-RP in a New Internetwork, page 45-26 (optional)
- Adding Auto-RP to an Existing Sparse-Mode Cloud, page 45-26 (optional)
- Preventing Join Messages to False RPs, page 45-28 (optional)
- Filtering Incoming RP Announcement Messages, page 45-29 (optional)

For overview information, see the “Auto-RP” section on page 45-6.

Setting up Auto-RP in a New Internetwork

If you are setting up Auto-RP in a new internetwork, you do not need a default RP because you configure all the interfaces for sparse-dense mode. Follow the process described in the “Adding Auto-RP to an Existing Sparse-Mode Cloud” section on page 45-26. However, omit Step 3 if you want to configure a PIM router as the RP for the local group.

Adding Auto-RP to an Existing Sparse-Mode Cloud

This section contains some suggestions for the initial deployment of Auto-RP into an existing sparse-mode cloud to minimize disruption of the existing multicast infrastructure.
Beginning in privileged EXEC mode, follow these steps to deploy Auto-RP in an existing sparse-mode cloud. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>show running-config</td>
<td>Verify that a default RP is already configured on all PIM devices and the RP in the sparse-mode network. It was previously configured with the <strong>ip pim rp-address</strong> global configuration command. This step is not required for sparse-dense-mode environments. The selected RP should have good connectivity and be available across the network. Use this RP for the global groups (for example 224.x.x.x and other global groups). Do not reconfigure the group address range that this RP serves. RPs dynamically discovered through Auto-RP take precedence over statically configured RPs. Assume that it is desirable to use a second RP for the local groups.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</td>
<td>Configure another PIM device to be the candidate RP for local groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <strong>interface-id</strong>, enter the interface type and number that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <strong>scope ttl</strong>, specify the time-to-live value in hops. Enter a hop count that is high enough so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <strong>group-list access-list-number</strong>, enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <strong>interval seconds</strong>, specify how often the announcement messages must be sent. The default is 60 seconds. The range is 1 to 16383.</td>
</tr>
<tr>
<td>4</td>
<td>access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <strong>access-list-number</strong>, enter the access list number specified in Step 3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <strong>deny</strong> keyword denies access if the conditions are matched. The <strong>permit</strong> keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <strong>source</strong>, enter the multicast group address range for which the RP should be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) For <strong>source-wildcard</strong>, 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>
</tr>
<tr>
<td></td>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
</tbody>
</table>
Chapter 45  Configuring IP Multicast Routing

Configuring IP Multicast Routing

To remove the PIM device configured as the candidate RP, use the `no ip pim send-rp-announce` global configuration command. To remove the switch as the RP-mapping agent, use the `no ip pim send-rp-discovery` global configuration command.

This example shows how to send RP announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address of port 1 is the RP. Access list 5 describes the group for which this switch serves as RP:

```
Switch(config)# ip pim send-rp-announce gigabitethernet0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

Preventing Join Messages to False RPs

Find whether the `ip pim accept-rp` command was previously configured throughout the network by using the `show running-config` privileged EXEC command. If the `ip pim accept-rp` command is not configured on any device, this problem can be addressed later. In those routers or multilayer switches already configured with the `ip pim accept-rp` command, you must enter the command again to accept the newly advertised RP.

To accept all RPs advertised with Auto-RP and reject all other RPs by default, use the `ip pim accept-rp auto-rp` global configuration command. This procedure is optional.

If all interfaces are in sparse mode, use a default-configured RP to support the two well-known groups 224.0.1.39 and 224.0.1.40. Auto-RP uses these two well-known groups to collect and distribute RP-mapping information. When this is the case and the `ip pim accept-rp auto-rp` command is configured, another `ip pim accept-rp` command accepting the RP must be configured as follows:

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```

Command Purpose

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>ip pim send-rp-discovery scope ttl</td>
<td>Find a switch whose connectivity is not likely to be interrupted, and assign it the role of RP-mapping agent. For <code>scope ttl</code>, specify the time-to-live value in hops to limit the RP discovery packets. All devices within the hop count from the source device receive the Auto-RP discovery messages. These messages tell other devices which group-to-RP mapping to use to avoid conflicts (such as overlapping group-to-RP ranges). There is no default setting. The range is 1 to 255.</td>
</tr>
<tr>
<td>6</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>show ip pim rp mapping</td>
<td>Display active RPs that are cached with associated multicast routing entries.</td>
</tr>
<tr>
<td></td>
<td>show ip pim rp</td>
<td>Display the information cached in the routing table.</td>
</tr>
<tr>
<td>8</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the PIM device configured as the candidate RP, use the `no ip pim send-rp-announce interface-id` global configuration command. To remove the switch as the RP-mapping agent, use the `no ip pim send-rp-discovery` global configuration command.

This example shows how to send RP announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address of port 1 is the RP. Access list 5 describes the group for which this switch serves as RP:

```
Switch(config)# ip pim send-rp-announce gigabitethernet0/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```
Filtering Incoming RP Announcement Messages

You can add configuration commands to the mapping agents to prevent a maliciously configured router from masquerading as a candidate RP and causing problems.

Beginning in privileged EXEC mode, follow these steps to filter incoming RP announcement messages. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip pim rp-announce-filter rp-list access-list-number group-list access-list-number</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove a filter on incoming RP announcement messages, use the **no ip pim rp-announce-filter rp-list access-list-number [group-list access-list-number]** global configuration command.
Configuring IP Multicast Routing

Chapter 45  Configuring IP Multicast Routing

This example shows a sample configuration on an Auto-RP mapping agent that is used to prevent candidate RP announcements from being accepted from unauthorized candidate RPs:

```
Switch(config) # ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config) # access-list 10 permit host 172.16.5.1
Switch(config) # access-list 10 permit host 172.16.2.1
Switch(config) # access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config) # access-list 20 permit 224.0.0.0 15.255.255.255
```

In this example, the mapping agent accepts candidate RP announcements from only two devices, 172.16.5.1 and 172.16.2.1. The mapping agent accepts candidate RP announcements from these two devices only for multicast groups that fall in the group range of 224.0.0.0 to 239.255.255.255. The mapping agent does not accept candidate RP announcements from any other devices in the network. Furthermore, the mapping agent does not accept candidate RP announcements from 172.16.5.1 or 172.16.2.1 if the announcements are for any groups in the 239.0.0.0 through 239.255.255.255 range. This range is the administratively scoped address range.

### Configuring PIMv2 BSR

These sections describe how to set up BSR in your PIMv2 network:

- Defining the PIM Domain Border, page 45-30 (optional)
- Defining the IP Multicast Boundary, page 45-31 (optional)
- Configuring Candidate BSRs, page 45-32 (optional)
- Configuring Candidate RPs, page 45-33 (optional)

For overview information, see the “Bootstrap Router” section on page 45-7.

### Defining the PIM Domain Border

As IP multicast becomes more widespread, the chance of one PIMv2 domain bordering another PIMv2 domain is increasing. Because these two domains probably do not share the same set of RPs, BSR, candidate RPs, and candidate BSRs, you need to constrain PIMv2 BSR messages from flowing into or out of the domain. Allowing these messages to leak across the domain borders could adversely affect the normal BSR election mechanism and elect a single BSR across all bordering domains and co-mingle candidate RP advertisements, resulting in the election of RPs in the wrong domain.

Beginning in privileged EXEC mode, follow these steps to define the PIM domain border. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip pim bsr-border</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
To remove the PIM border, use the `no ip pim bsr-border` interface configuration command.

**Figure 45-5 Constrainin g PIMv2 BSR Messages**

Defining the IP Multicast Boundary

You define a multicast boundary to prevent Auto-RP messages from entering the PIM domain. You create an access list to deny packets destined for 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.

Beginning in privileged EXEC mode, follow these steps to define a multicast boundary. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2  | `access-list access-list-number deny source [source-wildcard]` | Create a standard access list, repeating the command as many times as necessary.  
  - For `access-list-number`, the range is 1 to 99.  
  - The `deny` keyword denies access if the conditions are matched.  
  - For `source`, enter multicast addresses 224.0.1.39 and 224.0.1.40, which carry Auto-RP information.  
  - (Optional) For `source-wildcard`, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore.  
  Recall that the access list is always terminated by an implicit deny statement for everything. |
| Step 3  | `interface interface-id`         | Specify the interface to be configured, and enter interface configuration mode. |
| Step 4  | `ip multicast boundary access-list-number` | Configure the boundary, specifying the access list you created in Step 2. |
| Step 5  | `end`                            | Return to privileged EXEC mode.                                         |
| Step 6  | `show running-config`            | Verify your entries.                                                   |
| Step 7  | `copy running-config startup-config` | (Optional) Save your entries in the configuration file.                 |
To remove the boundary, use the `no ip multicast boundary` interface configuration command.

This example shows a portion of an IP multicast boundary configuration that denies Auto-RP information:

```bash
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# access-list 1 permit all
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip multicast boundary 1
```

**Configuring Candidate BSRs**

You can configure one or more candidate BSRs. The devices serving as candidate BSRs should have good connectivity to other devices and be in the backbone portion of the network.

Beginning in privileged EXEC mode, follow these steps to configure your switch as a candidate BSR. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>ip pim bsr-candidate interface-id hash-mask-length [priority]</code> Configure your switch to be a candidate BSR.</td>
</tr>
<tr>
<td></td>
<td>• For <code>interface-id</code>, enter the interface on this switch from which the BSR address is derived to make it a candidate. This interface must be enabled with PIM. Valid interfaces include physical ports, port channels, and VLANs.</td>
</tr>
<tr>
<td></td>
<td>• For <code>hash-mask-length</code>, specify the mask length (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>priority</code>, enter a number from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the device with the highest IP address is selected as the BSR. The default is 0.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show running-config</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove this device as a candidate BSR, use the `no ip pim bsr-candidate` global configuration command.

This example shows how to configure a candidate BSR, which uses the IP address 172.21.24.18 on a port as the advertised BSR address, uses 30 bits as the hash-mask-length, and has a priority of 10.

```bash
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip address 172.21.24.18 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip pim bsr-candidate gigabitethernet0/2 30 10
Switch(config-if)# ip pim bsr-candidate gigabitethernet1/2 30 10
```
Configuring Candidate RPs

You can configure one or more candidate RPs. Similar to BSRs, the RPs should also have good connectivity to other devices and be in the backbone portion of the network. An RP can serve the entire IP multicast address space or a portion of it. Candidate RPs send candidate RP advertisements to the BSR. When deciding which devices should be RPs, consider these options:

- In a network of Cisco routers and multilayer switches where only Auto-RP is used, any device can be configured as an RP.
- In a network that includes only Cisco PIMv2 routers and multilayer switches and with routers from other vendors, any device can be used as an RP.
- In a network of Cisco PIMv1 routers, Cisco PIMv2 routers, and routers from other vendors, configure only Cisco PIMv2 routers and multilayer switches as RPs.

Beginning in privileged EXEC mode, follow these steps to configure your switch to advertise itself as a PIMv2 candidate RP to the BSR. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip pim rp-candidate interface-id [group-list access-list-number]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>access-list access-list-number {deny</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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove this device as a candidate RP, use the `no ip pim rp-candidate interface-id` global configuration command.
This example shows how to configure the switch to advertise itself as a candidate RP to the BSR in its PIM domain. Standard access list number 4 specifies the group prefix associated with the RP that has the address identified by a port. That RP is responsible for the groups with the prefix 239.

Switch(config)# ip pim rp-candidate gigabitethernet0/2 group-list 4
Switch(config)# access-list 4 permit 239.0.0.0 0.255.255.255

Using Auto-RP and a BSR

If there are only Cisco devices in your network (no routers from other vendors), there is no need to configure a BSR. Configure Auto-RP in a network that is running both PIMv1 and PIMv2.

If you have non-Cisco PIMv2 routers that need to interoperate with Cisco PIMv1 routers and multilayer switches, both Auto-RP and a BSR are required. We recommend that a Cisco PIMv2 router or multilayer switch be both the Auto-RP mapping agent and the BSR.

If you must have one or more BSRs, we have these recommendations:

- Configure the candidate BSRs as the RP-mapping agents for Auto-RP. For more information, see the “Configuring Auto-RP” section on page 45-26 and the “Configuring Candidate BSRs” section on page 45-32.

- For group prefixes advertised through Auto-RP, the PIMv2 BSR mechanism should not advertise a subrange of these group prefixes served by a different set of RPs. In a mixed PIMv1 and PIMv2 domain, have backup RPs serve the same group prefixes. This prevents the PIMv2 DRs from selecting a different RP from those PIMv1 DRs, due to the longest match lookup in the RP-mapping database.

Beginning in privileged EXEC mode, follow these steps to verify the consistency of group-to-RP mappings. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><strong>show ip pim rp</strong></td>
<td>On any Cisco device, display the available RP mappings.</td>
</tr>
<tr>
<td>* [[group-name</td>
<td>(Optional) For <em>group-name</em>, specify the name of the group about which to display RPs.</td>
</tr>
<tr>
<td>]</td>
<td>(Optional) For <em>group-address</em>, specify the address of the group about which to display RPs.</td>
</tr>
<tr>
<td>* group-address]</td>
<td>(Optional) Use the <em>mapping</em> keyword to display all group-to-RP mappings of which the Cisco device is aware (configured or learned from Auto-RP).</td>
</tr>
<tr>
<td></td>
<td>(mapping)</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><strong>show ip pim rp-hash</strong></td>
<td>On a PIMv2 router or multilayer switch, confirm that the same RP is the one that a PIMv1 system chooses.</td>
</tr>
<tr>
<td>* group</td>
<td>For <em>group</em>, enter the group address for which to display RP information.</td>
</tr>
</tbody>
</table>

Monitoring the RP Mapping Information

To monitor the RP mapping information, use these commands in privileged EXEC mode:

- **show ip pim bsr** displays information about the elected BSR.
- **show ip pim rp-hash** displays the RP that was selected for the specified group.
- **show ip pim rp** [[group-name | (through the BSR or the Auto-RP mechanism). |
| ] * group-address] | displays how the switch learns of the RP (through the BSR or the Auto-RP mechanism). |
| * mapping] | | |
Troubleshooting PIMv1 and PIMv2 Interoperability Problems

When debugging interoperability problems between PIMv1 and PIMv2, check these in the order shown:

1. Verify RP mapping with the `show ip pim rp-hash` privileged EXEC command, making sure that all systems agree on the same RP for the same group.
2. Verify interoperability between different versions of DRs and RPs. Make sure the RPs are interacting with the DRs properly (by responding with register-stops and forwarding decapsulated data packets from registers).

Configuring Advanced PIM Features

These sections describe the optional advanced PIM features:
- Understanding PIM Shared Tree and Source Tree, page 45-35
- Delaying the Use of PIM Shortest-Path Tree, page 45-36 (optional)
- Modifying the PIM Router-Query Message Interval, page 45-37 (optional)

Understanding PIM Shared Tree and Source Tree

By default, members of a group receive data from senders to the group across a single data-distribution tree rooted at the RP. Figure 45-6 shows this type of shared-distribution tree. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

Figure 45-6  Shared Tree and Source Tree (Shortest-Path Tree)

If the data rate warrants, leaf routers (routers without any downstream connections) on the shared tree can use the data distribution tree rooted at the source. This type of distribution tree is called a shortest-path tree or source tree. By default, the software switches to a source tree upon receiving the first data packet from a source.
This process describes the move from a shared tree to a source tree:

1. A receiver joins a group; leaf Router C sends a join message toward the RP.
2. The RP puts a link to Router C in its outgoing interface list.
3. A source sends data; Router A encapsulates the data in a register message and sends it to the RP.
4. The RP forwards the data down the shared tree to Router C and sends a join message toward the source. At this point, data might arrive twice at Router C, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at the RP, it sends a register-stop message to Router A.
6. By default, reception of the first data packet prompts Router C to send a join message toward the source.
7. When Router C receives data on (S,G), it sends a prune message for the source up the shared tree.
8. The RP deletes the link to Router C from the outgoing interface of (S,G). The RP triggers a prune message toward the source.

Join and prune messages are sent for sources and RPs. They are sent hop-by-hop and are processed by each PIM device along the path to the source or RP. Register and register-stop messages are not sent hop-by-hop. They are sent by the designated router that is directly connected to a source and are received by the RP for the group.

Multiple sources sending to groups use the shared tree.

You can configure the PIM device to stay on the shared tree. For more information, see the “Delaying the Use of PIM Shortest-Path Tree” section on page 45-36.

### Delaying the Use of PIM Shortest-Path Tree

The change from shared to source tree happens when the first data packet arrives at the last-hop router (Router C in Figure 45-6). This change occurs because the `ip pim spt-threshold` global configuration command controls that timing.

The shortest-path tree requires more memory than the shared tree but reduces delay. You might want to postpone its use. Instead of allowing the leaf router to immediately move to the shortest-path tree, you can specify that the traffic must first reach a threshold.

You can configure when a PIM leaf router should join the shortest-path tree for a specified group. If a source sends at a rate greater than or equal to the specified kb/s rate, the multilayer switch triggers a PIM join message toward the source to construct a source tree (shortest-path tree). If the traffic rate from the source drops below the threshold value, the leaf router switches back to the shared tree and sends a prune message toward the source.

You can specify to which groups the shortest-path tree threshold applies by using a group list (a standard access list). If a value of 0 is specified or if the group list is not used, the threshold applies to all groups.
Beginning in privileged EXEC mode, follow these steps to configure a traffic rate threshold that must be reached before multicast routing is switched from the source tree to the shortest-path tree. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number [deny</td>
</tr>
<tr>
<td></td>
<td>Create a standard access list.</td>
</tr>
<tr>
<td></td>
<td>• For access-list-number, the range is 1 to 99.</td>
</tr>
<tr>
<td></td>
<td>• The deny keyword denies access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• The permit keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td></td>
<td>• For source, specify the multicast group to which the threshold applies.</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>
</tr>
<tr>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip pim spt-threshold {kbps</td>
</tr>
<tr>
<td></td>
<td>Specify the threshold that must be reached before moving to shortest-path tree (spt).</td>
</tr>
<tr>
<td></td>
<td>• For kbps, specify the traffic rate in kilobits per second. The default is 0 kb/s.</td>
</tr>
<tr>
<td></td>
<td>Note Because of switch hardware limitations, 0 kb/s is the only valid entry even though the range is 0 to 4294967.</td>
</tr>
<tr>
<td></td>
<td>• Specify infinity if you want all sources for the specified group to use the shared tree, never switching to the source tree.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For group-list access-list-number, specify the access list created in Step 2. If the value is 0 or if the group-list is not used, the threshold applies to all groups.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the no ip pim spt-threshold {kbps | infinity} global configuration command.

**Modifying the PIM Router-Query Message Interval**

PIM routers and multilayer switches send PIM router-query messages to find which device is the DR for each LAN segment (subnet). The DR is responsible for sending IGMP host-query messages to all hosts on the directly connected LAN.
With PIM DM operation, the DR has meaning only if IGMPv1 is in use. IGMPv1 does not have an IGMP querier election process, so the elected DR functions as the IGMP querier. With PIM SM operation, the DR is the device that is directly connected to the multicast source. It sends PIM register messages to notify the RP that multicast traffic from a source needs to be forwarded down the shared tree. In this case, the DR is the device with the highest IP address.

Beginning in privileged EXEC mode, follow these steps to modify the router-query message interval. This procedure is optional.

```
Step 1  configure terminal
Enter global configuration mode.
Step 2  interface interface-id
Specify the interface to be configured, and enter interface configuration mode.
Step 3  ip pim query-interval seconds
Configure the frequency at which the switch sends PIM router-query messages.
The default is 30 seconds. The range is 1 to 65535.
Step 4  end
Return to privileged EXEC mode.
Step 5  show ip igmp interface [interface-id]
Verify your entries.
Step 6  copy running-config startup-config
(Optional) Save your entries in the configuration file.
```

To return to the default setting, use the `no ip pim query-interval [seconds]` interface configuration command.

## Configuring Optional IGMP Features

These sections contain this configuration information:

- Default IGMP Configuration, page 45-39
- Configuring the Switch as a Member of a Group, page 45-39 (optional)
- Controlling Access to IP Multicast Groups, page 45-40 (optional)
- Changing the IGMP Version, page 45-41 (optional)
- Modifying the IGMP Host-Query Message Interval, page 45-41 (optional)
- Changing the IGMP Query Timeout for IGMPv2, page 45-42 (optional)
- Changing the Maximum Query Response Time for IGMPv2, page 45-43 (optional)
- Configuring the Switch as a Statically Connected Member, page 45-43 (optional)
Default IGMP Configuration

Table 45-4 shows the default IGMP configuration.

Table 45-4 Default IGMP Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multilayer switch as a member of a multicast group</td>
<td>No group memberships are defined.</td>
</tr>
<tr>
<td>Access to multicast groups</td>
<td>All groups are allowed on an interface.</td>
</tr>
<tr>
<td>IGMP version</td>
<td>Version 2 on all interfaces.</td>
</tr>
<tr>
<td>IGMP host-query message interval</td>
<td>60 seconds on all interfaces.</td>
</tr>
<tr>
<td>IGMP query timeout</td>
<td>60 seconds on all interfaces.</td>
</tr>
<tr>
<td>IGMP maximum query response time</td>
<td>10 seconds on all interfaces.</td>
</tr>
<tr>
<td>Multilayer switch as a statically connected member</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

Configuring the Switch as a Member of a Group

You can configure the switch as a member of a multicast group and discover multicast reachability in a network. If all the multicast-capable routers and multilayer switches that you administer are members of a multicast group, pinging that group causes all these devices to respond. The devices respond to ICMP echo-request packets addressed to a group of which they are members. Another example is the multicast trace-route tools provided in the software.

⚠️ Caution
Performing this procedure might impact the CPU performance because the CPU receives all data traffic for the group address.

Beginning in privileged EXEC mode, follow these steps to configure the switch to be a member of a group. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip igmp join-group group-address</code></td>
<td>Configure the switch to join a multicast group. By default, no group memberships are defined. For <code>group-address</code>, specify the multicast IP address in dotted decimal notation.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show ip igmp interface [interface-id]</code></td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To cancel membership in a group, use the no `ip igmp join-group group-address` interface configuration command.
This example shows how to enable the switch to join multicast group 255.2.2.2:

Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp join-group 255.2.2.2

Controlling Access to IP Multicast Groups

The switch sends IGMP host-query messages to find which multicast groups have members on attached local networks. The switch then forwards to these group members all packets addressed to the multicast group. You can place a filter on each interface to restrict the multicast groups that hosts on the subnet serviced by the interface can join.

Beginning in privileged EXEC mode, follow these steps to filter multicast groups allowed on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp access-group access-list-number</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
</tr>
<tr>
<td>Step 5</td>
<td>access-list access-list-number {deny</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></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>end</td>
</tr>
<tr>
<td>Step 7</td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td>Step 8</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To disable groups on an interface, use the no ip igmp access-group interface configuration command.

This example shows how to configure hosts attached to a port as able to join only group 255.2.2.2:

Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp access-group 1
Changing the IGMP Version

By default, the switch uses IGMP Version 2, which provides features such as the IGMP query timeout and the maximum query response time.

All systems on the subnet must support the same version. The switch does not automatically detect Version 1 systems and switch to Version 1. You can mix Version 1 and Version 2 hosts on the subnet because Version 2 routers or switches always work correctly with IGMPv1 hosts.

Configure the switch for Version 1 if your hosts do not support Version 2.

Beginning in privileged EXEC mode, follow these steps to change the IGMP version. This procedure is optional.

```
<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 ip igmp version 1</td>
<td>Specify the IGMP version that the switch uses.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show ip igmp interface [interface-id]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
```

To return to the default setting, use the **no ip igmp version** interface configuration command.

Modifying the IGMP Host-Query Message Interval

The switch periodically sends IGMP host-query messages to discover which multicast groups are present on attached networks. These messages are sent to the all-hosts multicast group (224.0.0.1) with a time-to-live (TTL) of 1. The switch sends host-query messages to refresh its knowledge of memberships present on the network. If, after some number of queries, the software discovers that no local hosts are members of a multicast group, the software stops forwarding multicast packets to the local network from remote origins for that group and sends a prune message upstream toward the source.

The switch elects a PIM designated router (DR) for the LAN (subnet). The DR is the router or multilayer switch with the highest IP address for IGMPv2. For IGMPv1, the DR is elected according to the multicast routing protocol that runs on the LAN. The designated router is responsible for sending IGMP host-query messages to all hosts on the LAN. In sparse mode, the designated router also sends PIM register and PIM join messages toward the RP router.
Beginning in privileged EXEC mode, follow these steps to modify the host-query interval. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip igmp query-interval seconds</td>
</tr>
</tbody>
</table>

Specify the interface to be configured, and enter interface configuration mode. Configure the frequency at which the designated router sends IGMP host-query messages. By default, the designated router sends IGMP host-query messages every 60 seconds to keep the IGMP overhead very low on hosts and networks. The range is 1 to 65535.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip igmp query-interval** interface configuration command.

### Changing the IGMP Query Timeout for IGMPv2

If you are using IGMPv2, you can specify the period of time before the switch takes over as the querier for the interface. By default, the switch waits twice the query interval controlled by the **ip igmp query-interval** interface configuration command. After that time, if the switch has received no queries, it becomes the querier.

You can configure the query interval by entering the **show ip igmp interface interface-id** privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to change the IGMP query timeout. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip igmp querier-timeout seconds</td>
</tr>
</tbody>
</table>

Specify the IGMP query timeout. The default is 60 seconds (twice the query interval). The range is 60 to 300.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

(Optional) Save your entries in the configuration file.

To return to the default setting, use the **no ip igmp querier-timeout** interface configuration command.
Changing the Maximum Query Response Time for IGMPv2

If you are using IGMPv2, you can change the maximum query response time advertised in IGMP queries. The maximum query response time enables the switch to quickly detect that there are no more directly connected group members on a LAN. Decreasing the value enables the switch to prune groups faster.

Beginning in privileged EXEC mode, follow these steps to change the maximum query response time. This procedure is optional.

To return to the default setting, use the `no ip igmp query-max-response-time` interface configuration command.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>ip igmp query-max-response-time seconds</td>
<td>Change the maximum query response time advertised in IGMP queries. The default is 10 seconds. The range is 1 to 25.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show ip igmp interface [interface-id]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Configuring the Switch as a Statically Connected Member

Sometimes there is either no group member on a network segment or a host cannot report its group membership by using IGMP. However, you might want multicast traffic to go to that network segment. These are ways to pull multicast traffic down to a network segment:

- Use the `ip igmp join-group` interface configuration command. With this method, the switch accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the switch from fast switching.
- Use the `ip igmp static-group` interface configuration command. With this method, the switch does not accept the packets itself, but only forwards them. This method enables fast switching. The outgoing interface appears in the IGMP cache, but the switch itself is not a member, as evidenced by lack of an L (local) flag in the multicast route entry.
Beginning in privileged EXEC mode, follow these steps to configure the switch itself to be a statically connected member of a group (and enable fast switching). This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip igmp static-group group-address</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ip igmp interface [interface-id]</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the switch as a member of the group, use the \texttt{no ip igmp static-group group-address} interface configuration command.

## Configuring Optional Multicast Routing Features

These sections describe how to configure optional multicast routing features:

- Features for Layer 2 connectivity and MBONE multimedia conference session and set up:
  - Enabling CGMP Server Support, page 45-44 (optional)
  - Configuring sdr Listener Support, page 45-45 (optional)
- Features that control bandwidth utilization:
  - Configuring an IP Multicast Boundary, page 45-47 (optional)
- Procedure for configuring a multicast within a VPN routing/forwarding (VRF) table:
  - Configuring Multicast VRFs, page 37-77

## Enabling CGMP Server Support

The switch serves as a CGMP server for devices that do not support IGMP snooping but have CGMP client functionality. CGMP is a protocol used on Cisco routers and multilayer switches connected to Layer 2 Catalyst switches to perform tasks similar to those performed by IGMP. CGMP is necessary because the Layer 2 switch cannot distinguish between IP multicast data packets and IGMP report messages, which are both at the MAC-level and are addressed to the same group address.
Beginning in privileged EXEC mode, follow these steps to enable the CGMP server on the switch interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface that is connected to the Layer 2 Catalyst switch, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 ip cgmp [proxy]</td>
<td>Enable CGMP on the interface. By default, CGMP is disabled on all interfaces. Enabling CGMP triggers a CGMP join message. Enable CGMP only on Layer 3 interfaces connected to Layer 2 Catalyst switches. (Optional) When you enter the proxy keyword, the CGMP proxy function is enabled. The proxy router advertises the existence of non-CGMP-capable routers by sending a CGMP join message with the non-CGMP-capable router MAC address and a group address of 0000.0000.0000.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Verify the Layer 2 Catalyst switch CGMP-client configuration. For more information, see the documentation that shipped with the product.</td>
</tr>
</tbody>
</table>

To disable CGMP on the interface, use the no ip cgmp interface configuration command.

When multiple Cisco CGMP-capable devices are connected to a switched network and the ip cgmp proxy command is needed, we recommend that all devices be configured with the same CGMP option and have precedence for becoming the IGMP querier over non-Cisco routers.

### Configuring sdr Listener Support

The MBONE is the small subset of Internet routers and hosts that are interconnected and capable of forwarding IP multicast traffic. Other multimedia content is often broadcast over the MBONE. Before you can join a multimedia session, you need to know what multicast group address and port are being used for the session, when the session is going to be active, and what sort of applications (audio, video, and so forth) are required on your workstation. The MBONE Session Directory Version 2 (sdr) tool provides this information. This freeware application can be downloaded from several sites on the World Wide Web, one of which is http://www.video.ja.net/mice/index.html.
SDR is a multicast application that listens to a well-known multicast group address and port for Session Announcement Protocol (SAP) multicast packets from SAP clients, which announce their conference sessions. These SAP packets contain a session description, the time the session is active, its IP multicast group addresses, media format, contact person, and other information about the advertised multimedia session. The information in the SAP packet is displayed in the SDR Session Announcement window.

### Enabling sdr Listener Support

By default, the switch does not listen to session directory advertisements. Beginning in privileged EXEC mode, follow these steps to enable the switch to join the default session directory group (224.2.127.254) on the interface and listen to session directory advertisements. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>Specify the interface to be enabled for sdr, and enter interface configuration mode.</td>
</tr>
<tr>
<td>ip sdr listen</td>
<td>Enable sdr listener support.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable sdr support, use the `no ip sdr listen` interface configuration command.

### Limiting How Long an sdr Cache Entry Exists

By default, entries are never deleted from the sdr cache. You can limit how long the entry remains active so that if a source stops advertising SAP information, old advertisements are not needlessly kept.

Beginning in privileged EXEC mode, follow these steps to limit how long an sdr cache entry stays active in the cache. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip sdr cache-timeout minutes</td>
<td>Limit how long an sdr cache entry stays active in the cache.</td>
</tr>
<tr>
<td></td>
<td>By default, entries are never deleted from the cache.</td>
</tr>
<tr>
<td></td>
<td>For minutes, the range is 1 to 4294967295.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no ip sdr cache-timeout` global configuration command. To delete the entire cache, use the `clear ip sdr` privileged EXEC command.

To display the session directory cache, use the `show ip sdr` privileged EXEC command.
Configuring an IP Multicast Boundary

Administratively-scoped boundaries can be used to limit the forwarding of multicast traffic outside of a domain or subdomain. This approach uses a special range of multicast addresses, called *administratively-scoped addresses*, as the boundary mechanism. If you configure an administratively-scoped boundary on a routed interface, multicast traffic whose multicast group addresses fall in this range can not enter or exit this interface, thereby providing a firewall for multicast traffic in this address range.

**Note**

Multicast boundaries and TTL thresholds control the scoping of multicast domains; however, TTL thresholds are not supported by the switch. You should use multicast boundaries instead of TTL thresholds to limit the forwarding of multicast traffic outside of a domain or a subdomain.

**Figure 45-7** shows that Company XYZ has an administratively-scoped boundary set for the multicast address range 239.0.0.0/8 on all routed interfaces at the perimeter of its network. This boundary prevents any multicast traffic in the range 239.0.0.0 through 239.255.255.255 from entering or leaving the network. Similarly, the engineering and marketing departments have an administratively-scoped boundary of 239.128.0.0/16 around the perimeter of their networks. This boundary prevents multicast traffic in the range of 239.128.0.0 through 239.128.255.255 from entering or leaving their respective networks.

**Figure 45-7**   *Administratively-Scoped Boundaries*

You can define an administratively-scoped boundary on a routed interface for multicast group addresses. A standard access list defines the range of addresses affected. When a boundary is defined, no multicast data packets are allowed to flow across the boundary from either direction. The boundary allows the same multicast group address to be reused in different administrative domains.

The IANA has designated the multicast address range 239.0.0.0 to 239.255.255.255 as the administratively-scoped addresses. This range of addresses can then be reused in domains administered by different organizations. The addresses would be considered local, not globally unique.
Beginning in privileged EXEC mode, follow these steps to set up an administratively-scoped boundary. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>access-list access-list-number {deny</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></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip multicast boundary access-list-number</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove the boundary, use the **no ip multicast boundary** interface configuration command.

This example shows how to set up a boundary for all administratively-scoped addresses:

Switch(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Switch(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip multicast boundary 1

### Configuring Basic DVMRP Interoperability Features

These sections contain this configuration information:

- Configuring DVMRP Interoperability, page 45-49 (optional)
- Configuring a DVMRP Tunnel, page 45-51 (optional)
- Advertising Network 0.0.0.0 to DVMRP Neighbors, page 45-52 (optional)
- Responding to mrinfo Requests, page 45-53 (optional)

For more advanced DVMRP features, see the “Configuring Advanced DVMRP Interoperability Features” section on page 45-53.
Configuring DVMRP Interoperability

Cisco multicast routers and multilayer switches using PIM can interoperate with non-Cisco multicast routers that use the DVMRP.

PIM devices dynamically discover DVMRP multicast routers on attached networks by listening to DVMR probe messages. When a DVMRP neighbor has been discovered, the PIM device periodically sends DVMRP report messages advertising the unicast sources reachable in the PIM domain. By default, directly connected subnets and networks are advertised. The device forwards multicast packets that have been forwarded by DVMRP routers and, in turn, forwards multicast packets to DVMRP routers.

You can configure an access list on the PIM routed interface connected to the MBONE to limit the number of unicast routes that are advertised in DVMRP route reports. Otherwise, all routes in the unicast routing table are advertised.

Note

The mrouted protocol is a public-domain implementation of DVMRP. You must use mrouted Version 3.8 (which implements a nonpruning version of DVMRP) when Cisco routers and multilayer switches are directly connected to DVMRP routers or interoperate with DVMRP routers over an MBONE tunnel. DVMRP advertisements produced by the Cisco IOS software can cause older versions of the mrouted protocol to corrupt their routing tables and those of their neighbors.

You can configure what sources are advertised and what metrics are used by configuring the ip dvmrp metric interface configuration command. You can also direct all sources learned through a particular unicast routing process to be advertised into DVMRP.

Beginning in privileged EXEC mode, follow these steps to configure the sources that are advertised and the metrics that are used when DVMRP route-report messages are sent. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]</td>
</tr>
<tr>
<td></td>
<td>• For access-list-number, the range is 1 to 99.</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>
</tr>
<tr>
<td></td>
<td>• For source, enter the number of the network or host from which the packet is being sent.</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>
</tr>
<tr>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Specify the interface connected to the MBONE and enabled for multicast routing, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
To disable the metric or route map, use the `no ip dvmrp metric metric [list access-list-number] [protocol process-id] | [dvmrp]]` or the `no ip dvmrp metric metric route-map map-name` command.

A more sophisticated way to achieve the same results as the preceding command is to use a route map (`ip dvmrp metric metric route-map map-name interface configuration command`) instead of an access list. You subject unicast routes to route-map conditions before they are injected into DVMRP.

This example shows how to configure DVMRP interoperability when the PIM device and the DVMRP router are on the same network segment. In this example, access list 1 advertises the networks (198.92.35.0, 198.92.36.0, 198.92.37.0, 131.108.0.0, and 150.136.0.0) to the DVMRP router, and access list 2 prevents all other networks from being advertised (`ip dvmrp metric 0 interface configuration command`).

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip address 131.119.244.244 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config-if)# ip dvmrp metric 1 list 1
Switch(config-if)# ip dvmrp metric 0 list 2
Switch(config-if)# exit
Switch(config)# access-list 1 permit 198.92.35.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.36.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
Switch(config)# access-list 1 permit 131.108.0.0 0.0.255.255
Switch(config)# access-list 1 permit 150.136.0.0 0.0.0.255
Switch(config)# access-list 1 deny 0.0.0.0 255.255.255.255
Switch(config)# access-list 2 permit 0.0.0.0 255.255.255.255
```
Configuring a DVMRP Tunnel

The software supports DVMRP tunnels to the MBONE. You can configure a DVMRP tunnel on a router or multilayer switch if the other end is running DVMRP. The software then sends and receives multicast packets through the tunnel. This strategy enables a PIM domain to connect to the DVMRP router when all routers on the path do not support multicast routing. You cannot configure a DVMRP tunnel between two routers.

When a Cisco router or multilayer switch runs DVMRP through a tunnel, it advertises sources in DVMRP report messages, much as it does on real networks. The software also caches DVMRP report messages it receives and uses them in its RPF calculation. This behavior enables the software to forward multicast packets received through the tunnel.

When you configure a DVMRP tunnel, you should assign an IP address to a tunnel in these cases:

- To send IP packets through the tunnel
- To configure the software to perform DVMRP summarization

The software does not advertise subnets through the tunnel if the tunnel has a different network number from the subnet. In this case, the software advertises only the network number through the tunnel.

Beginning in privileged EXEC mode, follow these steps to configure a DVMRP tunnel. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 access-list access-list-number [deny</td>
<td>Create a standard access list, repeating the command as many times as necessary.</td>
</tr>
<tr>
<td>permit] source [source-wildcard]</td>
<td>• For access-list-number, the range is 1 to 99.</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>
</tr>
<tr>
<td></td>
<td>• For source, enter the number of the network or host from which the packet is being sent.</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>
</tr>
<tr>
<td></td>
<td>Recall that the access list is always terminated by an implicit deny statement for everything.</td>
</tr>
<tr>
<td>Step 3 interface tunnel number</td>
<td>Specify a tunnel interface, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 4 tunnel source ip-address</td>
<td>Specify the source address of the tunnel interface. Enter the IP address of the interface on the switch.</td>
</tr>
<tr>
<td>Step 5 tunnel destination ip-address</td>
<td>Specify the destination address of the tunnel interface. Enter the IP address of the mrouted router.</td>
</tr>
<tr>
<td>Step 6 tunnel mode dvmrp</td>
<td>Configure the encapsulation mode for the tunnel to DVMRP.</td>
</tr>
<tr>
<td>Step 7 ip address address mask</td>
<td>Assign an IP address to the interface.</td>
</tr>
<tr>
<td>or</td>
<td>or</td>
</tr>
<tr>
<td>Step 8 ip unnumbered type number</td>
<td>Configure the interface as unnumbered.</td>
</tr>
<tr>
<td>Step 8 ip pim [dense-mode</td>
<td>sparse-mode]</td>
</tr>
</tbody>
</table>
Configuring Basic DVMRP Interoperability Features

Chapter 45 Configuring IP Multicast Routing

### Command Table

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|        | ip dvmrp accept-filter access-list-number [distance] neighbor-list access-list-number | Configure an acceptance filter for incoming DVMRP reports. By default, all destination reports are accepted with a distance of 0. Reports from all neighbors are accepted.  
- For **access-list-number**, specify the access list number created in Step 2. Any sources that match the access list are stored in the DVMRP routing table with distance.  
- (Optional) For **distance**, enter the administrative distance to the destination. By default, the administrative distance for DVMRP routes is 0 and take precedence over unicast routing table routes. If you have two paths to a source, one through unicast routing (using PIM as the multicast routing protocol) and another using DVMRP, and if you want to use the PIM path, increase the administrative distance for DVMRP routes. The range is 1 to 255.  
- For **neighbor-list access-list-number**, enter the number of the neighbor list created in Step 2. DVMRP reports are accepted only by those neighbors on the list. |
| Step 10 | end | Return to privileged EXEC mode. |
| Step 11 | show running-config | Verify your entries. |
| Step 12 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable the filter, use the **no ip dvmrp accept-filter access-list-number [distance] neighbor-list access-list-number** interface configuration command.

This example shows how to configure a DVMRP tunnel. In this configuration, the IP address of the tunnel on the Cisco switch is assigned *unnumbered*, which causes the tunnel to appear to have the same IP address as port 1. The tunnel endpoint source address is 172.16.2.1, and the tunnel endpoint address of the remote DVMRP router to which the tunnel is connected is 192.168.1.10. Any packets sent through the tunnel are encapsulated in an outer IP header. The Cisco switch is configured to accept incoming DVMRP reports with a distance of 100 from 198.92.37.0 through 198.92.37.255.

```
Switch(config)# ip multicast-routing
Switch(config)# interface tunnel 0
Switch(config-if)# ip unnumbered gigabitethernet0/1
Switch(config-if)# ip pim dense-mode
Switch(config-if)# tunnel source gigabitethernet0/1
Switch(config-if)# tunnel destination 192.168.1.10
Switch(config-if)# tunnel mode dvmrp
Switch(config-if)# ip dvmrp accept-filter 1 100
Switch(config-if)# ip address 172.16.2.1 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config)# exit
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
```

### Advertising Network 0.0.0.0 to DVMRP Neighbors

If your switch is a neighbor of an mrouted Version 3.6 device, you can configure the software to advertise network 0.0.0.0 (the default route) to the DVMRP neighbor. The DVMRP default route computes the RPF information for any multicast sources that do not match a more specific route.

Do not advertise the DVMRP default into the MBONE.
Beginning in privileged EXEC mode, follow these steps to advertise network 0.0.0.0 to DVMRP neighbors on an interface. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the interface that is connected to the DVMRP router, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| 3    | ip dvmrp default-information {originator | only} | Advertise network 0.0.0.0 to DVMRP neighbors. Use this command only when the switch is a neighbor of mrouted Version 3.6 machines. The keywords have these meanings:  
- **originator**—Specifies that other routes more specific than 0.0.0.0 can also be advertised.  
- **only**—Specifies that no DVMRP routes other than 0.0.0.0 are advertised. |
| 4    | end | Return to privileged EXEC mode. |
| 5    | show running-config | Verify your entries. |
| 6    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To prevent the default route advertisement, use the **no ip dvmrp default-information** interface configuration command.

**Responding to mrinfo Requests**

The software answers mrinfo requests sent by mrouted systems and Cisco routers and multilayer switches. The software returns information about neighbors through DVMRP tunnels and all the routed interfaces. This information includes the metric (always set to 1), the configured TTL threshold, the status of the interface, and various flags. You can also use the **mrinfo** privileged EXEC command to query the router or switch itself, as in this example:

```
Switch# mrinfo  
171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:  
171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]  
171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]  
171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]  
171.69.214.37 -> 0.0.0.0 [1/0/pim/querier/down/leaf]  
171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]  
171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]  
171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]  
171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

**Configuring Advanced DVMRP Interoperability Features**

Cisco routers and multilayer switches run PIM to forward multicast packets to receivers and receive multicast packets from senders. It is also possible to propagate DVMRP routes into and through a PIM cloud. PIM uses this information; however, Cisco routers and multilayer switches do not implement DVMRP to forward multicast packets.
These sections contain this configuration information:

- Enabling DVMRP Unicast Routing, page 45-54 (optional)
- Rejecting a DVMRP Nonpruning Neighbor, page 45-55 (optional)
- Controlling Route Exchanges, page 45-57 (optional)

For information on basic DVMRP features, see the “Configuring Basic DVMRP Interoperability Features” section on page 45-48.

### Enabling DVMRP Unicast Routing

Because multicast routing and unicast routing require separate topologies, PIM must follow the multicast topology to build loopless distribution trees. Using DVMRP unicast routing, Cisco routers, multilayer switches, and mrouted-based machines exchange DVMRP unicast routes, to which PIM can then reverse-path forward.

Cisco devices do not perform DVMRP multicast routing among each other, but they can exchange DVMRP routes. The DVMRP routes provide a multicast topology that might differ from the unicast topology. This enables PIM to run over the multicast topology, thereby enabling sparse-mode PIM over the MBONE topology.

When DVMRP unicast routing is enabled, the router or switch caches routes learned in DVMRP report messages in a DVMRP routing table. When PIM is running, these routes might be preferred over routes in the unicast routing table, enabling PIM to run on the MBONE topology when it is different from the unicast topology.

DVMRP unicast routing can run on all interfaces. For DVMRP tunnels, it uses DVMRP multicast routing. This feature does not enable DVMRP multicast routing among Cisco routers and multilayer switches. However, if there is a DVMRP-capable multicast router, the Cisco device can do PIM/DVMRP multicast routing.

Beginning in privileged EXEC mode, follow these steps to enable DVMRP unicast routing. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specify the interface that is connected to the DVMRP router, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip dvmrp unicast-routing</td>
<td>Enable DVMRP unicast routing (to send and receive DVMRP routes). This feature is disabled by default.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To disable this feature, use the `no ip dvmrp unicast-routing` interface configuration command.
Rejecting a DVMRP Nonpruning Neighbor

By default, Cisco devices accept all DVMRP neighbors as peers, regardless of their DVMRP capability. However, some non-Cisco devices run old versions of DVMRP that cannot prune, so they continuously receive forwarded packets, wasting bandwidth. Figure 45-8 shows this scenario.

*Figure 45-8  Leaf Nonpruning DVMRP Neighbor*

You can prevent the switch from peering (communicating) with a DVMRP neighbor if that neighbor does not support DVMRP pruning or grafting. To do so, configure the switch (which is a neighbor to the leaf, nonpruning DVMRP machine) with the `ip dvmrp reject-non-pruners` interface configuration command on the interface connected to the nonpruning machine as shown in Figure 45-9. In this case, when the switch receives DVMRP probe or report message without the prune-capable flag set, the switch logs a syslog message and discards the message.
Note that the `ip dvmrp reject-non-pruners` interface configuration command prevents peering with neighbors only. If there are any nonpruning routers multiple hops away (downstream toward potential receivers) that are not rejected, a nonpruning DVMRP network might still exist.

Beginning in privileged EXEC mode, follow these steps to prevent peering with nonpruning DVMRP neighbors. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip dvmrp reject-non-pruners</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>end</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>show running-config</code></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code></td>
</tr>
</tbody>
</table>

To disable this function, use the `no ip dvmrp reject-non-pruners` interface configuration command.
Controlling Route Exchanges

These sections describe how to tune the Cisco device advertisements of DVMRP routes:

- Limiting the Number of DVMRP Routes Advertised, page 45-57 (optional)
- Changing the DVMRP Route Threshold, page 45-57 (optional)
- Configuring a DVMRP Summary Address, page 45-58 (optional)
- Disabling DVMRP Autosummarization, page 45-60 (optional)
- Adding a Metric Offset to the DVMRP Route, page 45-60 (optional)

Limiting the Number of DVMRP Routes Advertised

By default, only 7000 DVMRP routes are advertised over an interface enabled to run DVMRP (that is, a DVMRP tunnel, an interface where a DVMRP neighbor has been discovered, or an interface configured to run the `ip dvmrp unicast-routing` interface configuration command).

Beginning in privileged EXEC mode, follow these steps to change the DVMRP route limit. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip dvmrp route-limit count</td>
<td>Change the number of DVMRP routes advertised over an interface enabled for DVMRP.</td>
</tr>
<tr>
<td></td>
<td>This command prevents misconfigured <code>ip dvmrp metric</code> interface configuration commands from causing massive route injection into the MBONE.</td>
</tr>
<tr>
<td></td>
<td>By default, 7000 routes are advertised. The range is 0 to 4294967295.</td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To configure no route limit, use the `no ip dvmrp route-limit` global configuration command.

Changing the DVMRP Route Threshold

By default, 10,000 DVMRP routes can be received per interface within a 1-minute interval. When that rate is exceeded, a syslog message is issued, warning that there might be a route surge occurring. The warning is typically used to quickly detect when devices have been misconfigured to inject a large number of routes into the MBONE.
Beginning in privileged EXEC mode, follow these steps to change the threshold number of routes that trigger the warning. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip dvmrp routehog-notification route-count</td>
<td>Configure the number of routes that trigger a syslog message. The default is 10,000 routes. The range is 1 to 4294967295.</td>
</tr>
<tr>
<td>Step 3 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 5 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting use the **no ip dvmrp routehog-notification** global configuration command.

Use the **show ip igmp interface** privileged EXEC command to display a running count of routes. When the count is exceeded, ***ALERT*** is appended to the line.

### Configuring a DVMRP Summary Address

By default, a Cisco device advertises in DVMRP route-report messages only connected unicast routes (that is, only routes to subnets that are directly connected to the router) from its unicast routing table. These routes undergo normal DVMRP classful route summarization. This process depends on whether the route being advertised is in the same classful network as the interface over which it is being advertised.

**Figure 45-10** shows an example of the default behavior. This example shows that the DVMRP report sent by the Cisco router contains the three original routes received from the DVMRP router that have been poison-reversed by adding 32 to the DVMRP metric. Listed after these routes are two routes that are advertisements for the two directly connected networks (176.32.10.0/24 and 176.32.15.0/24) that were taken from the unicast routing table. Because the DVMRP tunnel shares the same IP address as Fast Ethernet port 1 and falls into the same Class B network as the two directly connected subnets, classful summarization of these routes was not performed. As a result, the DVMRP router is able to poison-reverse only these two routes to the directly connected subnets and is able to only RPF properly for multicast traffic sent by sources on these two Ethernet segments. Any other multicast source in the network behind the Cisco router that is not on these two Ethernet segments does not properly RPF-check on the DVMRP router and is discarded.

You can force the Cisco router to advertise the summary address (specified by the address and mask pair in the **ip dvmrp summary-address address mask** interface configuration command) in place of any route that falls in this address range. The summary address is sent in a DVMRP route report if the unicast routing table contains at least one route in this range; otherwise, the summary address is not advertised. In **Figure 45-10**, you configure the **ip dvmrp summary-address** command on the Cisco router tunnel interface. As a result, the Cisco router sends only a single summarized Class B advertisement for network 176.32.0.0.16 from the unicast routing table.
Beginning in privileged EXEC mode, follow these steps to customize the summarization of DVMRP routes if the default classful autosummarization does not suit your needs. This procedure is optional.

**Note**  
At least one more-specific route must be present in the unicast routing table before a configured summary address is advertised.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
</tbody>
</table>
| Step 3  | ip dvmrp summary-address address mask [metric value] | Specify a DVMRP summary address.  
- For summary-address address mask, specify the summary IP address and mask that is advertised instead of the more specific route.  
- (Optional) For metric value, specify the metric that is advertised with the summary address. The default is 1. The range is 1 to 32. |
| Step 4  | end | Return to privileged EXEC mode. |
| Step 5  | show running-config | Verify your entries. |
| Step 6  | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To remove the summary address, use the no ip dvmrp summary-address address mask [metric value] interface configuration command.
Disabling DVMRP Autosummarization

By default, the software automatically performs some level of DVMRP summarization. Disable this function if you want to advertise all routes, not just a summary. In some special cases, you can use the neighboring DVMRP router with all subnet information to better control the flow of multicast traffic in the DVMRP network. One such case might occur if the PIM network is connected to the DVMRP cloud at several points and more specific (unsummarized) routes are being injected into the DVMRP network to advertise better paths to individual subnets inside the PIM cloud.

If you configure the `ip dvmrp summary-address` interface configuration command and did not configure `no ip dvmrp auto-summary`, you get both custom and autosummaries.

Beginning in privileged EXEC mode, follow these steps to disable DVMRP autosummarization. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>no ip dvmrp auto-summary</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To re-enable auto summarization, use the `ip dvmrp auto-summary` interface configuration command.

Adding a Metric Offset to the DVMRP Route

By default, the switch increments by one the metric (hop count) of a DVMRP route advertised in incoming DVMRP reports. You can change the metric if you want to favor or not favor a certain route.

For example, a route is learned by multilayer switch A, and the same route is learned by multilayer switch B with a higher metric. If you want to use the path through switch B because it is a faster path, you can apply a metric offset to the route learned by switch A to make it larger than the metric learned by switch B, and you can choose the path through switch B.
Beginning in privileged EXEC mode, follow these steps to change the default metric. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the interface to be configured, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 ip dvmrp metric-offset [in</td>
<td>out] increment</td>
</tr>
<tr>
<td></td>
<td>The keywords have these meanings:</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>in</strong>—Specifies that the increment value is added to incoming DVMRP reports and is reported in mrinfo replies.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) <strong>out</strong>—Specifies that the increment value is added to outgoing DVMRP reports for routes from the DVMRP routing table.</td>
</tr>
<tr>
<td></td>
<td>If neither <strong>in</strong> nor <strong>out</strong> is specified, <strong>in</strong> is the default.</td>
</tr>
<tr>
<td></td>
<td>For <strong>increment</strong>, specify the value that is added to the metric of a DVMRP router advertised in a report message. The range is 1 to 31. If the <strong>ip dvmrp metric-offset</strong> command is not configured on an interface, the default increment value for incoming routes is 1, and the default for outgoing routes is 0.</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no ip dvmrp metric-offset** interface configuration command.

**Monitoring and Maintaining IP Multicast Routing**

These sections describe how to monitor and maintain IP multicast routing:

- Clearing Caches, Tables, and Databases, page 45-62
- Displaying System and Network Statistics, page 45-62
- Monitoring IP Multicast Routing, page 45-63
Clearing Caches, Tables, and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database might be necessary when the contents of the particular structure are or suspected to be invalid.

You can use any of the privileged EXEC commands in Table 45-5 to clear IP multicast caches, tables, and databases:

<table>
<thead>
<tr>
<th>Table 45-5 Commands for Clearing Caches, Tables, and Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>clear ip cgmp</td>
</tr>
<tr>
<td>clear ip dvmrp route { *</td>
</tr>
<tr>
<td>clear ip igmp group [ group-name</td>
</tr>
<tr>
<td>clear ip mroute { *</td>
</tr>
<tr>
<td>clear ip pim auto-rp rp-address</td>
</tr>
<tr>
<td>clear ip sdr [ group-address</td>
</tr>
</tbody>
</table>

Displaying System and Network Statistics

You can display specific statistics, such as the contents of IP routing tables, caches, and databases.

This release does not support per-route statistics.

You can display information to learn resource usage and solve network problems. You can also display information about node reachability and discover the routing path that packets of your device are taking through the network.

You can use any of the privileged EXEC commands in Table 45-6 to display various routing statistics:

<table>
<thead>
<tr>
<th>Table 45-6 Commands for Displaying System and Network Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>ping [ group-name</td>
</tr>
<tr>
<td>show ip dvmrp route [ ip-address ]</td>
</tr>
<tr>
<td>show ip igmp groups [ group-name</td>
</tr>
<tr>
<td>show ip igmp interface [ type number ]</td>
</tr>
</tbody>
</table>
### Table 45-6 Commands for Displaying System and Network Statistics (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip mpacket</code> [source-address</td>
<td>name] [group-address</td>
</tr>
<tr>
<td><code>show ip mroute</code> [group-name</td>
<td>group-address] [source] [summary] [count] [active kbps]</td>
</tr>
<tr>
<td><code>show ip pim interface</code> [type number] [count] [detail]</td>
<td>Display information about interfaces configured for PIM. This command is available in all software images.</td>
</tr>
<tr>
<td><code>show ip pim neighbor</code> [type number]</td>
<td>List the PIM neighbors discovered by the switch. This command is available in all software images.</td>
</tr>
<tr>
<td><code>show ip pim rp</code> [group-name</td>
<td>group-address]</td>
</tr>
<tr>
<td><code>show ip rpf</code> [source-address</td>
<td>name]</td>
</tr>
</tbody>
</table>

### Monitoring IP Multicast Routing

You can use the privileged EXEC commands in Table 45-7 to monitor IP multicast routers, packets, and paths:

### Table 45-7 Commands for Monitoring IP Multicast Routing

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mrinfo</code> [hostname</td>
<td>address] [source-address</td>
</tr>
<tr>
<td><code>mstat</code> source [destination] [group]</td>
<td>Display IP multicast packet rate and loss information.</td>
</tr>
<tr>
<td><code>mtrace</code> source [destination] [group]</td>
<td>Trace the path from a source to a destination branch for a multicast distribution tree for a given group.</td>
</tr>
</tbody>
</table>
This chapter describes how to configure the Multicast Source Discovery Protocol (MSDP) on the Catalyst 3560 switch. The MSDP connects multiple Protocol-Independent Multicast sparse-mode (PIM-SM) domains.

MSDP is not fully supported in this software release because of a lack of support for Multicast Border Gateway Protocol (MBGP), which works closely with MSDP. However, it is possible to create default peers that MSDP can operate with if MBGP is not running.

To use this feature, the switch must be running the IP services image.

For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2* from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Understanding MSDP, page 46-1
- Configuring MSDP, page 46-3
- Monitoring and Maintaining MSDP, page 46-18

### Understanding MSDP

MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and does not depend on RPs in other domains. An RP runs MSDP over the Transmission Control Protocol (TCP) to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled devices in another domain. The peering relationship occurs over a TCP connection, primarily exchanging a list of sources sending to multicast groups. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM. MSDP is also used to announce sources sending to a group. These announcements must originate at the domain’s RP.
MSDP depends heavily on the Border Gateway Protocol (BGP) or MBGP for interdomain operation. We recommend that you run MSDP in RPs in your domain that are RPs for sources sending to global groups to be announced to the Internet.

**MSDP Operation**

Figure 46-1 shows MSDP operating between two MSDP peers. PIM uses MSDP as the standard mechanism to register a source with the RP of a domain. When MSDP is configured, this sequence occurs.

When a source sends its first multicast packet, the first-hop router (designated router or RP) directly connected to the source sends a PIM register message to the RP. The RP uses the register message to register the active source and to forward the multicast packet down the shared tree in the local domain. With MSDP configured, the RP also forwards a source-active (SA) message to all MSDP peers. The SA message identifies the source, the group the source is sending to, and the address of the RP or the originator ID (the IP address of the interface used as the RP address), if configured.

Each MSDP peer receives and forwards the SA message away from the originating RP to achieve peer reverse-path flooding (RPF). The MSDP device examines the BGP or MBGP routing table to discover which peer is the next hop toward the originating RP of the SA message. Such a peer is called an RPF peer (reverse-path forwarding peer). The MSDP device forwards the message to all MSDP peers other than the RPF peer. For information on how to configure an MSDP peer when BGP and MBGP are not supported, see the “Configuring a Default MSDP Peer” section on page 46-4.

If the MSDP peer receives the same SA message from a non-RPF peer toward the originating RP, it drops the message. Otherwise, it forwards the message to all its MSDP peers.

The RP for a domain receives the SA message from an MSDP peer. If the RP has any join requests for the group the SA message describes and if the (*,G) entry exists with a nonempty outgoing interface list, the domain is interested in the group, and the RP triggers an (S,G) join toward the source. After the (S,G) join reaches the source’s DR, a branch of the source tree has been built from the source to the RP in the remote domain. Multicast traffic can now flow from the source across the source tree to the RP and then down the shared tree in the remote domain to the receiver.
MSDP Benefits

MSDP has these benefits:

- It breaks up the shared multicast distribution tree. You can make the shared tree local to your domain. Your local members join the local tree, and join messages for the shared tree never need to leave your domain.
- PIM sparse-mode domains can rely only on their own RPs, decreasing reliance on RPs in another domain. This increases security because you can prevent your sources from being known outside your domain.
- Domains with only receivers can receive data without globally advertising group membership.
- Global source multicast routing table state is not required, saving memory.

Configuring MSDP

These sections contain this configuration information:

- Default MSDP Configuration, page 46-4
- Configuring a Default MSDP Peer, page 46-4 (required)
- Caching Source-Active State, page 46-6 (optional)
- Requesting Source Information from an MSDP Peer, page 46-8 (optional)
• Controlling Source Information that Your Switch Originates, page 46-8 (optional)
• Controlling Source Information that Your Switch Forwards, page 46-11 (optional)
• Controlling Source Information that Your Switch Receives, page 46-13 (optional)
• Configuring an MSDP Mesh Group, page 46-15 (optional)
• Shutting Down an MSDP Peer, page 46-15 (optional)
• Including a Bordering PIM Dense-Mode Region in MSDP, page 46-16 (optional)
• Configuring an Originating Address other than the RP Address, page 46-17 (optional)

Default MSDP Configuration

MSDP is not enabled, and no default MSDP peer exists.

Configuring a Default MSDP Peer

In this software release, because BGP and MBGP are not supported, you cannot configure an MSDP peer on the local switch by using the `ip msdp peer` global configuration command. Instead, you define a default MSDP peer (by using the `ip msdp default-peer` global configuration command) from which to accept all SA messages for the switch. The default MSDP peer must be a previously configured MSDP peer. Configure a default MSDP peer when the switch is not BGP- or MBGP-peering with an MSDP peer. If a single MSDP peer is configured, the switch always accepts all SA messages from that peer.

Figure 46-2 shows a network in which default MSDP peers might be used. In Figure 46-2, a customer who owns Switch B is connected to the Internet through two Internet service providers (ISPs), one owning Router A and the other owning Router C. They are not running BGP or MBGP between them. To learn about sources in the ISP’s domain or in other domains, Switch B at the customer site identifies Router A as its default MSDP peer. Switch B advertises SA messages to both Router A and Router C but accepts SA messages only from Router A or only from Router C. If Router A is first in the configuration file, it is used if it is running. If Router A is not running, only then does Switch B accept SA messages from Router C. This is the default behavior without a prefix list.

If you specify a prefix list, the peer is a default peer only for the prefixes in the list. You can have multiple active default peers when you have a prefix list associated with each. When you do not have any prefix lists, you can configure multiple default peers, but only the first one is the active default peer as long as the router has connectivity to this peer and the peer is alive. If the first configured peer fails or the connectivity to this peer fails, the second configured peer becomes the active default, and so on.

The ISP probably uses a prefix list to define which prefixes it accepts from the customer’s router.
Beginning in privileged EXEC mode, follow these steps to specify a default MSDP peer. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| **Step 2** `ip msdp default-peer ip-address | name [prefix-list list]` | Define a default peer from which to accept all MSDP SA messages.  
  - For `ip-address | name`, enter the IP address or Domain Name System (DNS) server name of the MSDP default peer.  
  - (Optional) For `prefix-list list`, enter the list name that specifies the peer to be the default peer only for the listed prefixes. You can have multiple active default peers when you have a prefix list associated with each.  

When you enter multiple `ip msdp default-peer` commands with the `prefix-list` keyword, you use all the default peers at the same time for different RP prefixes. This syntax is typically used in a service provider cloud that connects stub site clouds.  

When you enter multiple `ip msdp default-peer` commands without the `prefix-list` keyword, a single active peer accepts all SA messages. If that peer fails, the next configured default peer accepts all SA messages. This syntax is typically used at a stub site.
Configuring MSDP

To remove the default peer, use the `no ip msdp default-peer ip-address | name` global configuration command.

This example shows a partial configuration of Router A and Router C in Figure 46-2. Each of these ISPs have more than one customer (like the customer in Figure 46-2) who use default peering (no BGP or MBGP). In that case, they might have similar configurations. That is, they accept SAs only from a default peer if the SA is permitted by the corresponding prefix list.

**Router A**

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

**Router C**

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

### Caching Source-Active State

By default, the switch does not cache source/group pairs from received SA messages. When the switch forwards the MSDP SA information, it does not store it in memory. Therefore, if a member joins a group soon after a SA message is received by the local RP, that member needs to wait until the next SA message to hear about the source. This delay is known as join latency.

If you want to sacrifice some memory in exchange for reducing the latency of the source information, you can configure the switch to cache SA messages.

---

**Step 3**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip prefix-list name [description string]</td>
<td>seq number [permit</td>
</tr>
<tr>
<td></td>
<td>• (Optional) For <code>description string</code>, enter a description of up to 80 characters to describe this prefix list.</td>
</tr>
<tr>
<td></td>
<td>• For <code>seq number</code>, enter the sequence number of the entry. The range is 1 to 4294967294.</td>
</tr>
<tr>
<td></td>
<td>• The <code>deny</code> keyword denies access to matching conditions.</td>
</tr>
<tr>
<td></td>
<td>• The <code>permit</code> keyword permits access to matching conditions.</td>
</tr>
<tr>
<td></td>
<td>• For <code>network length</code>, specify the network number and length (in bits) of the network mask that is permitted or denied.</td>
</tr>
</tbody>
</table>

**Step 4**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip msdp description {peer-name</td>
<td>peer-address} text`</td>
</tr>
<tr>
<td></td>
<td>By default, no description is associated with an MSDP peer.</td>
</tr>
</tbody>
</table>

**Step 5**

```
end
```

Return to privileged EXEC mode.

**Step 6**

```
show running-config
```

Verify your entries.

**Step 7**

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

(Optional) Save your entries in the configuration file.
Beginning in privileged EXEC mode, follow these steps to enable the caching of source/group pairs. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip msdp cache-sa-state [list access-list-number]</td>
</tr>
<tr>
<td>Step 3</td>
<td>access-list access-list-number {deny</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></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>end</td>
</tr>
<tr>
<td>Step 5</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

An alternative to this command is the `ip msdp sa-request` global configuration command, which causes the switch to send an SA request message to the MSDP peer when a new member for a group becomes active. For more information, see the next section.

To return to the default setting (no SA state is created), use the `no ip msdp cache-sa-state` global configuration command.

This example shows how to enable the cache state for all sources in 171.69.0.0/16 sending to groups 224.2.0.0/16:

```
Switch(config)# ip msdp cache-sa-state 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```
Requesting Source Information from an MSDP Peer

Local RPs can send SA requests and get immediate responses for all active sources for a given group. By default, the switch does not send any SA request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive the next periodic SA message.

If you want a new member of a group to learn the active multicast sources in a connected PIM sparse-mode domain that are sending to a group, configure the switch to send SA request messages to the specified MSDP peer when a new member joins a group. The peer replies with the information in its SA cache. If the peer does not have a cache configured, this command has no result. Configuring this feature reduces join latency but sacrifices memory.

Beginning in privileged EXEC mode, follow these steps to configure the switch to send SA request messages to the MSDP peer when a new member joins a group and wants to receive multicast traffic. This procedure is optional.

To return to the default setting, use the `no ip msdp sa-request {ip-address | name}` global configuration command.

This example shows how to configure the switch to send SA request messages to the MSDP peer at 171.69.1.1:

```
Switch(config)# ip msdp sa-request 171.69.1.1
```

**Controlling Source Information that Your Switch Originates**

You can control the multicast source information that originates with your switch:

- Sources you advertise (based on your sources)
- Receivers of source information (based on knowing the requestor)

For more information, see the “Redistributing Sources” section on page 46-9 and the “Filtering Source-Active Request Messages” section on page 46-10.
**Redistributing Sources**

SA messages originate on RPs to which sources have registered. By default, any source that registers with an RP is advertised. The *A flag* is set in the RP when a source is registered, which means the source is advertised in an SA unless it is filtered.

Beginning in privileged EXEC mode, follow these steps to further restrict which registered sources are advertised. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</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>
</tbody>
</table>
Configuring MSDP

Filtering Source-Active Request Messages

By default, only switches that are caching SA information can respond to SA requests. By default, such a switch honors all SA request messages from its MSDP peers and supplies the IP addresses of the active sources.

However, you can configure the switch to ignore all SA requests from an MSDP peer. You can also honor only those SA request messages from a peer for groups described by a standard access list. If the groups in the access list pass, SA request messages are accepted. All other such messages from the peer for other groups are ignored.

To remove the filter, use the `no ip msdp redistribute` global configuration command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`access-list access-list-number {deny</td>
<td>permit} source [source-wildcard]<code>or</code>access-list access-list-number {deny</td>
</tr>
<tr>
<td><em>For <code>access-list-number</code>, the range is 1 to 99 for standard access lists and 100 to 199 for extended lists. Enter the same number created in Step 2.</em></td>
<td></td>
</tr>
<tr>
<td><em>The <code>deny</code> keyword denies access if the conditions are matched. The <code>permit</code> keyword permits access if the conditions are matched.</em></td>
<td></td>
</tr>
<tr>
<td><em>For <code>protocol</code>, enter <code>ip</code> as the protocol name.</em></td>
<td></td>
</tr>
<tr>
<td><em>For <code>source</code>, enter the number of the network or host from which the packet is being sent.</em></td>
<td></td>
</tr>
<tr>
<td><em>For <code>source-wildcard</code>, 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.</em></td>
<td></td>
</tr>
<tr>
<td><em>For <code>destination</code>, enter the number of the network or host to which the packet is being sent.</em></td>
<td></td>
</tr>
<tr>
<td><em>For <code>destination-wildcard</code>, enter the wildcard bits in dotted decimal notation to be applied to the destination. Place ones in the bit positions that you want to ignore.</em></td>
<td></td>
</tr>
<tr>
<td><em>Recall that the access list is always terminated by an implicit deny statement for everything.</em></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Verify your entries.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps to configure one of these options. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>`ip msdp filter-sa-request ip-address</td>
</tr>
<tr>
<td></td>
<td>name`</td>
</tr>
<tr>
<td></td>
<td>`ip msdp filter-sa-request {ip-address</td>
</tr>
<tr>
<td></td>
<td>name} list access-list-number`</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>`access-list access-list-number {deny</td>
</tr>
<tr>
<td></td>
<td>permit} source [source-wildcard]`</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></td>
<td></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></td>
<td></td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no ip msdp filter-sa-request {ip-address` global configuration command.

This example shows how to configure the switch to filter SA request messages from the MSDP peer at 171.69.2.2. SA request messages from sources on network 192.4.22.0 pass access list 1 and are accepted; all others are ignored.

<table>
<thead>
<tr>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Switch(config)# ip msdp filter sa-request 171.69.2.2 list 1</code></td>
<td><code>Switch(config)# access-list 1 permit 192.4.22.0 0.0.0.255</code></td>
</tr>
</tbody>
</table>

**Controlling Source Information that Your Switch Forwards**

By default, the switch forwards all SA messages it receives to all its MSDP peers. However, you can prevent outgoing messages from being forwarded to a peer by using a filter or by setting a time-to-live (TTL) value. These methods are described in the next sections.
## Using a Filter

By creating a filter, you can perform one of these actions:

- Filter all source/group pairs
- Specify an IP extended access list to pass only certain source/group pairs
- Filter based on match criteria in a route map

Beginning in privileged EXEC mode, follow these steps to apply a filter. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>**ip msdp sa-filter out ip-address</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**access-list access-list-number {deny</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
</tbody>
</table>
To remove the filter, use the `no ip msdp sa-filter out {ip-address | name} [list access-list-number] [route-map map-tag]` global configuration command.

This example shows how to allow only (S,G) pairs that pass access list 100 to be forwarded in an SA message to the peer named `switch.cisco.com`:

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter out switch.cisco.com list 100
Switch(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

### Using TTL to Limit the Multicast Data Sent in SA Messages

You can use a TTL value to control what data is encapsulated in the first SA message for every source. Only multicast packets with an IP-header TTL greater than or equal to the `ttl` argument are sent to the specified MSDP peer. For example, you can limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you must send those packets with a TTL greater than 8.

Beginning in privileged EXEC mode, follow these steps to establish a TTL threshold. This procedure is optional.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>ip msdp ttl-threshold {ip-address</td>
<td>name} ttl</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For `ip-address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>ttl</code>, enter the TTL value. The default is 0, which means all multicast data packets are forwarded to the peer until the TTL is exhausted. The range is 0 to 255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the `no ip msdp ttl-threshold {ip-address | name}` global configuration command.

### Controlling Source Information that Your Switch Receives

By default, the switch receives all SA messages that its MSDP RPF peers send to it. However, you can control the source information that you receive from MSDP peers by filtering incoming SA messages. In other words, you can configure the switch to not accept them.
You can perform one of these actions:
- Filter all incoming SA messages from an MSDP peer
- Specify an IP extended access list to pass certain source/group pairs
- Filter based on match criteria in a route map

Beginning in privileged EXEC mode, follow these steps to apply a filter. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>ip msdp sa-filter in ip-address</td>
</tr>
<tr>
<td>or</td>
<td>name</td>
</tr>
<tr>
<td>or</td>
<td>ip msdp sa-filter in {ip-address</td>
</tr>
<tr>
<td>list access-list-number</td>
<td>If both the list and the route-map keywords are used, all conditions must be true to pass any (S,G) pair in incoming SA messages.</td>
</tr>
<tr>
<td>or</td>
<td>ip msdp sa-filter in {ip-address</td>
</tr>
<tr>
<td>name } route-map map-tag</td>
<td>If all match criteria are true, a permit from the route map passes routes through the filter. A deny will filter routes.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>access-list access-list-number {deny</td>
</tr>
<tr>
<td>permit} protocol source source-wildcard</td>
<td>• For access-list-number, enter the number specified in Step 2.</td>
</tr>
<tr>
<td>destination destination-wildcard</td>
<td>• The deny keyword denies access if the conditions are matched. The permit keyword permits access if the conditions are matched.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
To remove the filter, use the `no ip msdp sa-filter in {ip-address | name} [list access-list-number] [route-map map-tag]` global configuration command.

This example shows how to filter all SA messages from the peer named `switch.cisco.com`:

```
Switch(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet0/1
Switch(config)# ip msdp sa-filter in switch.cisco.com
```

### Configuring an MSDP Mesh Group

An MSDP mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among one another. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. Thus, you reduce SA message flooding and simplify peer-RPF flooding. Use the `ip msdp mesh-group` global configuration command when there are multiple RPs within a domain. It is especially used to send SA messages across a domain. You can configure multiple mesh groups (with different names) in a single switch.

Beginning in privileged EXEC mode, follow these steps to create a mesh group. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>`ip msdp mesh-group name {ip-address</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>show running-config</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Repeat this procedure on each MSDP peer in the group.</td>
</tr>
</tbody>
</table>

To remove an MSDP peer from a mesh group, use the `no ip msdp mesh-group name {ip-address | name}` global configuration command.

### Shutting Down an MSDP Peer

If you want to configure many MSDP commands for the same peer and you do not want the peer to become active, you can shut down the peer, configure it, and later bring it up. When a peer is shut down, the TCP connection is terminated and is not restarted. You can also shut down an MSDP session without losing configuration information for the peer.
Beginning in privileged EXEC mode, follow these steps to shut down a peer. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip msdp shutdown {peer-name</td>
</tr>
<tr>
<td>Step 3</td>
<td>end</td>
</tr>
<tr>
<td>Step 4</td>
<td>show running-config</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To bring the peer back up, use the **no ip msdp shutdown {peer-name | peer address}** global configuration command. The TCP connection is reestablished.

### Including a Bordering PIM Dense-Mode Region in MSDP

You can configure MSDP on a switch that borders a PIM sparse-mode region with a dense-mode region. By default, active sources in the dense-mode region do not participate in MSDP.

**Note**

We do not recommend using the **ip msdp border sa-address** global configuration command. It is better to configure the border router in the sparse-mode domain to proxy-register sources in the dense-mode domain to the RP of the sparse-mode domain and have the sparse-mode domain use standard MSDP procedures to advertise these sources.

Beginning in privileged EXEC mode, follow these steps to configure the border router to send SA messages for sources active in the dense-mode region to the MSDP peers. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip msdp border sa-address interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map]</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
</tbody>
</table>
Chapter 46 Configuring MSDP

Note that the `ip msdp originator-id` global configuration command also identifies an interface to be used as the RP address. If both the `ip msdp border sa-address` and the `ip msdp originator-id` global configuration commands are configured, the address derived from the `ip msdp originator-id` command specifies the RP address.

To return to the default setting (active sources in the dense-mode region do not participate in MSDP), use the `no ip msdp border sa-address interface-id` global configuration command.

Configuring an Originating Address other than the RP Address

You can allow an MSDP speaker that originates an SA message to use the IP address of the interface as the RP address in the SA message by changing the Originator ID. You might change the Originator ID in one of these cases:

- If you configure a logical RP on multiple switches in an MSDP mesh group.
- If you have a switch that borders a PIM sparse-mode domain and a dense-mode domain. If a switch borders a dense-mode domain for a site, and sparse-mode is being used externally, you might want dense-mode sources to be known to the outside world. Because this switch is not an RP, it would not have an RP address to use in an SA message. Therefore, this command provides the RP address by specifying the address of the interface.

Beginning in privileged EXEC mode, follow these steps to allow an MSDP speaker that originates an SA message to use the IP address on the interface as the RP address in the SA message. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td><code>show running-config</code> Verify your entries.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>copy running-config startup-config</code> (Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

If both the `ip msdp border sa-address` and the `ip msdp originator-id` global configuration commands are configured, the address derived from the `ip msdp originator-id` command specifies the address of the RP.

To prevent the RP address from being derived in this way, use the `no ip msdp originator-id interface-id` global configuration command.
Monitoring and Maintaining MSDP

To monitor MSDP SA messages, peers, state, or peer status, use one or more of the privileged EXEC commands in Table 46-1:

**Table 46-1 Commands for Monitoring and Maintaining MSDP**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ip msdp [peer-address</td>
<td>Debugs an MSDP activity.</td>
</tr>
<tr>
<td>name] [detail] [routes]</td>
<td></td>
</tr>
<tr>
<td>debug ip msdp resets</td>
<td>Debugs MSDP peer reset reasons.</td>
</tr>
<tr>
<td>show ip msdp count [autonomous-system-number]</td>
<td>Displays the number of sources and groups originated in SA messages from each autonomous system. The <code>ip msdp cache-sa-state</code> command must be configured for this command to produce any output.</td>
</tr>
<tr>
<td>show ip msdp peer [peer-address</td>
<td>Displays detailed information about an MSDP peer.</td>
</tr>
<tr>
<td>name]</td>
<td></td>
</tr>
<tr>
<td>show ip msdp sa-cache [group-address</td>
<td>Displays (S,G) state learned from MSDP peers.</td>
</tr>
<tr>
<td>source-address</td>
<td></td>
</tr>
<tr>
<td>group-name</td>
<td></td>
</tr>
<tr>
<td>source-name</td>
<td></td>
</tr>
<tr>
<td>autonomous-system-number</td>
<td></td>
</tr>
<tr>
<td>show ip msdp summary</td>
<td>Displays MSDP peer status and SA message counts.</td>
</tr>
</tbody>
</table>

To clear MSDP connections, statistics, or SA cache entries, use the privileged EXEC commands in Table 46-2:

**Table 46-2 Commands for Clearing MSDP Connections, Statistics, or SA Cache Entries**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip msdp peer peer-address</td>
<td>Clears the TCP connection to the specified MSDP peer, resetting all MSDP message counters.</td>
</tr>
<tr>
<td>name</td>
<td></td>
</tr>
<tr>
<td>clear ip msdp statistics peer-address</td>
<td>Clears statistics counters for one or all the MSDP peers without resetting the sessions.</td>
</tr>
<tr>
<td>name</td>
<td></td>
</tr>
<tr>
<td>clear ip msdp sa-cache group-address</td>
<td>Clears the SA cache entries for all entries, all sources for a specific group, or all entries for a specific source/group pair.</td>
</tr>
<tr>
<td>name</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Fallback Bridging

This chapter describes how to configure fallback bridging (VLAN bridging) on the Catalyst 3560 switch. With fallback bridging, you can forward non-IP packets that the switch does not route between VLAN bridge domains and routed ports.

To use this feature, the switch must be running the IP services image. For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Understanding Fallback Bridging, page 47-1
- Configuring Fallback Bridging, page 47-3
- Monitoring and Maintaining Fallback Bridging, page 47-10

Understanding Fallback Bridging

With fallback bridging, the switch bridges together two or more VLANs or routed ports, essentially connecting multiple VLANs within one bridge domain. Fallback bridging forwards traffic that the switch does not route and forwards traffic belonging to a nonroutable protocol such as DECnet.

A VLAN bridge domain is represented with switch virtual interfaces (SVIs). A set of SVIs and routed ports (which do not have any VLANs associated with them) can be configured (grouped together) to form a bridge group. Recall that an SVI represents a VLAN of switch ports as one interface to the routing or bridging function in the system. You associate only one SVI with a VLAN, and you configure an SVI for a VLAN only when you want to route between VLANs, to fallback-bridge nonroutable protocols between VLANs, or to provide IP host connectivity to the switch. A routed port is a physical port that acts like a port on a router, but it is not connected to a router. A routed port is not associated with a particular VLAN, does not support VLAN subinterfaces, but behaves like a normal routed port. For more information about SVIs and routed ports, see Chapter 11, “Configuring Interface Characteristics.”

A bridge group is an internal organization of network interfaces on a switch. You cannot use bridge groups to identify traffic switched within the bridge group outside the switch on which they are defined. Bridge groups on the switch function as distinct bridges; that is, bridged traffic and bridge protocol data units (BPDUs) are not exchanged between different bridge groups on a switch.
Fallback bridging does not allow the spanning trees from the VLANs being bridged to collapse. Each VLAN has its own spanning-tree instance and a separate spanning tree, called the VLAN-bridge spanning tree, which runs on top of the bridge group to prevent loops.

The switch creates a VLAN-bridge spanning-tree instance when a bridge group is created. The switch runs the bridge group and treats the SVIs and routed ports in the bridge group as its spanning-tree ports.

These are the reasons for placing network interfaces into a bridge group:

- To bridge all nonrouted traffic among the network interfaces making up the bridge group. If the packet destination address is in the bridge table, the packet is forwarded on a single interface in the bridge group. If the packet destination address is not in the bridge table, the packet is flooded on all forwarding interfaces in the bridge group. A source MAC address is learned on a bridge group only when the address is learned on a VLAN (the reverse is not true).

- To participate in the spanning-tree algorithm by receiving, and in some cases sending, BPDUs on the LANs to which they are attached. A separate spanning-tree process runs for each configured bridge group. Each bridge group participates in a separate spanning-tree instance. A bridge group establishes a spanning-tree instance based on the BPDUs it receives on only its member interfaces. If the bridge STP BPDU is received on a port whose VLAN does not belong to a bridge group, the BPDU is flooded on all the forwarding ports of the VLAN.

**Figure 47-1** shows a fallback bridging network example. The switch has two ports configured as SVIs with different assigned IP addresses and attached to two different VLANs. Another port is configured as a routed port with its own IP address. If all three of these ports are assigned to the same bridge group, non-IP protocol frames can be forwarded among the end stations connected to the switch even though they are on different networks and in different VLANs. IP addresses do not need to be assigned to routed ports or SVIs for fallback bridging to work.

**Figure 47-1  Fallback Bridging Network Example**
Configuring Fallback Bridging

These sections contain this configuration information:

- Default Fallback Bridging Configuration, page 47-3
- Fallback Bridging Configuration Guidelines, page 47-3
- Creating a Bridge Group, page 47-4 (required)
- Adjusting Spanning-Tree Parameters, page 47-5 (optional)

Default Fallback Bridging Configuration

Table 47-1 shows the default fallback bridging configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge groups</td>
<td>None are defined or assigned to a port. No VLAN-bridge STP is defined.</td>
</tr>
<tr>
<td>Switch forwards frames for stations that it has dynamically learned</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Spanning tree parameters:</td>
<td></td>
</tr>
<tr>
<td>• Switch priority</td>
<td>• 32768.</td>
</tr>
<tr>
<td>• Port priority</td>
<td>• 128.</td>
</tr>
<tr>
<td>• Port path cost</td>
<td>• 10 Mb/s: 100.</td>
</tr>
<tr>
<td>• Hello BPDU interval</td>
<td>• 100 Mb/s: 19.</td>
</tr>
<tr>
<td>• Forward-delay interval</td>
<td>• 1000 Mb/s: 4.</td>
</tr>
<tr>
<td>• Maximum idle interval</td>
<td>• 2 seconds.</td>
</tr>
<tr>
<td></td>
<td>• 20 seconds.</td>
</tr>
<tr>
<td></td>
<td>• 30 seconds.</td>
</tr>
</tbody>
</table>

Fallback Bridging Configuration Guidelines

Up to 32 bridge groups can be configured on the switch.

An interface (an SVI or routed port) can be a member of only one bridge group.

Use a bridge group for each separately bridged (topologically distinct) network connected to the switch.

Do not configure fallback bridging on a switch configured with private VLANs.

All protocols except IP (Version 4 and Version 6), Address Resolution Protocol (ARP), reverse ARP (RARP), LOOPBACK, Frame Relay ARP, and shared STP packets are fallback bridged.
Creating a Bridge Group

To configure fallback bridging for a set of SVIs or routed ports, these interfaces must be assigned to bridge groups. All interfaces in the same group belong to the same bridge domain. Each SVI or routed port can be assigned to only one bridge group.

Note

The protected port feature is not compatible with fallback bridging. When fallback bridging is enabled, it is possible for packets to be forwarded from one protected port on a switch to another protected port on the same switch if the ports are in different VLANs.

Beginning in privileged EXEC mode, follow these steps to create a bridge group and to assign an interface to it. This procedure is required.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>bridge bridge-group protocol vlan-bridge</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bridge-group bridge-group</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show running-config</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

To remove a bridge group, use the no bridge bridge-group global configuration command. The no bridge bridge-group command automatically removes all SVIs and routes ports from that bridge group. To remove an interface from a bridge group and to remove the bridge group, use the no bridge-group bridge-group interface configuration command.
This example shows how to create bridge group 10, to specify that the VLAN-bridge STP runs in the bridge group, to define a port as a routed port, and to assign the port to the bridge group:

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# no shutdown
Switch(config-if)# bridge-group 10
```

This example shows how to create bridge group 10 and to specify that the VLAN-bridge STP runs in the bridge group. It defines an SVI for VLAN 2 and assigns it to the bridge group:

```
Switch(config)# bridge 10 protocol vlan-bridge
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# interface vlan2
Switch(config-if)# bridge-group 10
Switch(config-if)# exit
```

### Adjusting Spanning-Tree Parameters

You might need to adjust certain spanning-tree parameters if the default values are not suitable. You configure parameters affecting the entire spanning tree by using variations of the `bridge` global configuration command. You configure interface-specific parameters by using variations of the `bridge-group` interface configuration command.

You can adjust spanning-tree parameters by performing any of the tasks in these sections:

- Changing the VLAN-Bridge Spanning-Tree Priority, page 47-5 (optional)
- Changing the Interface Priority, page 47-6 (optional)
- Assigning a Path Cost, page 47-7 (optional)
- Adjusting BPDU Intervals, page 47-7 (optional)
- Disabling the Spanning Tree on an Interface, page 47-9 (optional)

**Note**

Only network administrators with a good understanding of how switches and STP function should make adjustments to spanning-tree parameters. Poorly planned adjustments can have a negative impact on performance. A good source on switching is the IEEE 802.1D specification. For more information, see the “References and Recommended Reading” appendix in the *Cisco IOS Configuration Fundamentals Command Reference*.

### Changing the VLAN-Bridge Spanning-Tree Priority

You can globally configure the VLAN-bridge spanning-tree priority of a switch when it ties with another switch for the position as the root switch. You also can configure the likelihood that the switch will be selected as the root switch.
Beginning in privileged EXEC mode, follow these steps to change the switch priority. This procedure is optional.

**Command** | **Purpose**
--- | ---
**Step 1** | configure terminal Enter global configuration mode.
**Step 2** | bridge bridge-group priority number Change the VLAN-bridge spanning-tree priority of the switch.
  - For *bridge-group*, specify the bridge group number. The range is 1 to 255.
  - For *number*, enter a number from 0 to 65535. The default is 32768. The lower the number, the more likely the switch will be chosen as the root.
**Step 3** | end Return to privileged EXEC mode.
**Step 4** | show running-config Verify your entry.
**Step 5** | copy running-config startup-config (Optional) Save your entry in the configuration file.

To return to the default setting, use the **no bridge bridge-group priority** global configuration command.

To change the priority on a port, use the **bridge-group priority** interface configuration command (described in the next section).

This example shows how to set the switch priority to 100 for bridge group 10:

```
Switch(config)# bridge 10 priority 100
```

### Changing the Interface Priority

You can change the priority for a port. When two switches tie for position as the root switch, you configure a port priority to break the tie. The switch with the lowest interface value is elected.

Beginning in privileged EXEC mode, follow these steps to change the interface priority. This procedure is optional.

**Command** | **Purpose**
--- | ---
**Step 1** | configure terminal Enter global configuration mode.
**Step 2** | interface interface-id Specify the interface to set the priority, and enter interface configuration mode.
**Step 3** | bridge-group bridge-group priority number Change the priority of a port.
  - For *bridge-group*, specify the bridge group number. The range is 1 to 255.
  - For *number*, enter a number from 0 to 255 in increments of 4. The lower the number, the more likely that the port on the switch will be chosen as the root. The default is 128.
**Step 4** | end Return to privileged EXEC mode.
**Step 5** | show running-config Verify your entry.
**Step 6** | copy running-config startup-config (Optional) Save your entry in the configuration file.
To return to the default setting, use the `no bridge-group bridge-group priority` interface configuration command.

This example shows how to change the priority to 20 on a port in bridge group 10:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# bridge-group 10 priority 20
```

### Assigning a Path Cost

Each port has a path cost associated with it. By convention, the path cost is 1000/data rate of the attached LAN, in Mb/s.

Beginning in privileged EXEC mode, follow these steps to assign a path cost. This procedure is optional.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specify the port to set the path cost, and enter interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>bridge-group bridge-group path-cost cost</td>
<td>Assign the path cost of a port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>bridge-group</code>, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For <code>cost</code>, enter a number from 0 to 65535. The higher the value, the higher the cost.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– For 10 Mb/s, the default path cost is 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– For 100 Mb/s, the default path cost is 19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– For 1000 Mb/s, the default path cost is 4.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show running-config</td>
<td>Verify your entry.</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default path cost, use the `no bridge-group bridge-group path-cost` interface configuration command.

This example shows how to change the path cost to 20 on a port in bridge group 10:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# bridge-group 10 path-cost 20
```

### Adjusting BPDU Intervals

You can adjust BPDU intervals as described in these sections:

- Adjusting the Interval between Hello BPDU s, page 47-8 (optional)
- Changing the Forward-Delay Interval, page 47-8 (optional)
- Changing the Maximum-Idle Interval, page 47-9 (optional)
Configuring Fallback Bridging

Adjusting the Interval between Hello BPDUs

Beginning in privileged EXEC mode, follow these step to adjust the interval between hello BPDUs. This procedure is optional.

### Adjusting the Interval between Hello BPDUs

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>bridge bridge-group hello-time seconds</strong> Specify the interval between hello BPDUs.</td>
</tr>
<tr>
<td></td>
<td>* For <em>bridge-group</em>, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>* For <em>seconds</em>, enter a number from 1 to 10. The default is 2.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>show running-config</strong> Verify your entry.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>copy running-config startup-config</strong> (Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

To return to the default setting, use the **no bridge bridge-group hello-time** global configuration command.

This example shows how to change the hello interval to 5 seconds in bridge group 10:

```
Switch(config)# bridge 10 hello-time 5
```

Changing the Forward-Delay Interval

The forward-delay interval is the amount of time spent listening for topology change information after a port has been activated for switching and before forwarding actually begins.

Beginning in privileged EXEC mode, follow these steps to change the forward-delay interval. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>bridge bridge-group forward-time seconds</strong> Specify the forward-delay interval.</td>
</tr>
<tr>
<td></td>
<td>* For <em>bridge-group</em>, specify the bridge group number. The range is 1 to 255.</td>
</tr>
<tr>
<td></td>
<td>* For <em>seconds</em>, enter a number from 4 to 200. The default is 20.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>end</strong> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>show running-config</strong> Verify your entry.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>copy running-config startup-config</strong> (Optional) Save your entry in the configuration file.</td>
</tr>
</tbody>
</table>

Command Purpose

**Step 1** **configure terminal** Enter global configuration mode.

**Step 2** **bridge bridge-group forward-time seconds** Specify the forward-delay interval.

* For **bridge-group**, specify the bridge group number. The range is 1 to 255.

* For **seconds**, enter a number from 4 to 200. The default is 20.

**Step 3** **end** Return to privileged EXEC mode.

**Step 4** **show running-config** Verify your entry.

**Step 5** **copy running-config startup-config** (Optional) Save your entry in the configuration file.
To return to the default setting, use the **no bridge bridge-group forward-time** global configuration command.

This example shows how to change the forward-delay interval to 10 seconds in bridge group 10:

```
Switch(config)# bridge 10 forward-time 10
```

### Changing the Maximum-Idle Interval

If a switch does not receive BPDUs from the root switch within a specified interval, it recomputes the spanning-tree topology.

Beginning in privileged EXEC mode, follow these steps to change the maximum-idle interval (maximum aging time). This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 2  | `bridge bridge-group max-age seconds` Specify the interval that the switch waits to hear BPDUs from the root switch.  
          - For `bridge-group`, specify the bridge group number. The range is 1 to 255.  
          - For `seconds`, enter a number from 6 to 200. The default is 30. |
| Step 3  | `end` Return to privileged EXEC mode. |
| Step 4  | `show running-config` Verify your entry. |
| Step 5  | `copy running-config startup-config` (Optional) Save your entry in the configuration file. |

To return to the default setting, use the **no bridge bridge-group max-age** global configuration command.

This example shows how to change the maximum-idle interval to 30 seconds in bridge group 10:

```
Switch(config)# bridge 10 max-age 30
```

### Disabling the Spanning Tree on an Interface

When a loop-free path exists between any two switched subnetworks, you can prevent BPDUs generated in one switching subnetwork from impacting devices in the other switching subnetwork, yet still permit switching throughout the network as a whole. For example, when switched LAN subnetworks are separated by a WAN, BPDUs can be prevented from traveling across the WAN link.

Beginning in privileged EXEC mode, follow these steps to disable spanning tree on a port. This procedure is optional.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface-id</code> Specify the port, and enter interface configuration mode.</td>
</tr>
</tbody>
</table>
| Step 3  | `bridge-group bridge-group spanning-disabled` Disable spanning tree on the port.  
          For `bridge-group`, specify the bridge group number. The range is 1 to 255. |
| Step 4  | `end` Return to privileged EXEC mode. |
To re-enable spanning tree on the port, use the `no bridge-group bridge-group spanning-disabled` interface configuration command.

This example shows how to disable spanning tree on a port in bridge group 10:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# bridge group 10 spanning-disabled
```

### Monitoring and Maintaining Fallback Bridging

To monitor and maintain the network, use one or more of the privileged EXEC commands in Table 47-2:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear bridge bridge-group</code></td>
<td>Removes any learned entries from the forwarding database.</td>
</tr>
<tr>
<td><code>show bridge [bridge-group] group</code></td>
<td>Displays details about the bridge group.</td>
</tr>
<tr>
<td>`show bridge [bridge-group] [interface-id</td>
<td>mac-address</td>
</tr>
</tbody>
</table>

For information about the fields in these displays, see the *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2, Release 12.2* from the Cisco.com page under **Documentation > Cisco IOS Software > 12.2 Mainline > Command References**.
Troubleshooting

This chapter describes how to identify and resolve software problems related to the Cisco IOS software on the Catalyst 3560 switch. Depending on the nature of the problem, you can use the command-line interface (CLI), the device manager, or Network Assistant to identify and solve problems.

Additional troubleshooting information, such as LED descriptions, is provided in the hardware installation guide.

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release and the Cisco IOS Commands Master List, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This chapter consists of these sections:

- Recovering from a Software Failure, page 48-2
- Recovering from a Lost or Forgotten Password, page 48-3
- Recovering from a Command Switch Failure, page 48-7
- Recovering from Lost Cluster Member Connectivity, page 48-11

Note Recovery procedures require that you have physical access to the switch.

- Preventing Autonegotiation Mismatches, page 48-11
- Troubleshooting Power over Ethernet Switch Ports, page 48-11
- SFP Module Security and Identification, page 48-12
- Monitoring SFP Module Status, page 48-13
- Monitoring Temperature, page 48-13
- Using Ping, page 48-13
- Using Layer 2 Traceroute, page 48-14
- Using IP Traceroute, page 48-16
- Using TDR, page 48-18
- Using Debug Commands, page 48-19
- Using the show platform forward Command, page 48-20
- Using the crashinfo Files, page 48-23
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 to and extract the bin file.

- If you are using UNIX, follow these steps:
  1. Display the contents of the tar file by using the `tar -tvf `*image_filename.tar*` UNIX command.

  `unix-1% tar -tvf image_filename.tar`

  `2. Locate the bin file, and extract it by using the `tar -xvf `*image_filename.tar*` <image_filename.bin>` UNIX command.`

  `unix-1% tar -xvf image_filename.tar image_filename.bin`

  x c3560-ipservices-mz.122-25.SEB/c3560-ipservices-mz.122-25.SEB.bin, 3970586 bytes, 7756 tape blocks`

  3. Verify that the bin file was extracted by using the `ls -l` *image_filename.bin*` UNIX command.

  `unix-1% ls -l image_filename.bin`

  `-rw-r--r-- 1 boba 3970586 Apr 21 12:00 c3560-ipservices-mz.122-25.SEB/c3560-ipservices-mz.122-25.SEB.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:

```
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```
Recovering from a Lost or Forgotten Password

The default configuration for the switch allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process during power-on and by entering a new password. These recovery procedures require that you have physical access to the switch.

On these switches, a system administrator can disable some of the functionality of this feature by allowing an end user to reset a password only by agreeing to return to the default configuration. If you are an end user trying to reset a password when password recovery has been disabled, a status message shows this during the recovery process.

These sections describes how to recover a forgotten or lost switch password:
- Procedure with Password Recovery Enabled, page 48-4
- Procedure with Password Recovery Disabled, page 48-6

You enable or disable password recovery by using the `service password-recovery` global configuration command. Follow the steps in this procedure if you have forgotten or lost the switch password.

Step 1 Connect a terminal or PC with terminal-emulation software to the switch console port.
Step 2 Set the line speed on the emulation software to 9600 baud.
Step 3 Power off the switch.
Recovering from a Lost or Forgotten Password

Chapter 48  Troubleshooting

Recovering from a Lost or Forgotten Password

Step 4  Reconnect the power cord to the switch and, within 15 seconds, press the **Mode** button while the System LED is still flashing green. Continue pressing the **Mode** button until the System LED turns briefly amber and then solid green; 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:**
  
  The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system
  
  go to the “Procedure with Password Recovery Enabled” section on page 48-4, and follow the steps.

- **If you see a message that begins with this:**
  
  The password-recovery mechanism has been triggered, but is currently disabled.
  
  go to the “Procedure with Password Recovery Disabled” section on page 48-6, and follow the steps.

Step 5  After recovering the password, reload the switch:

```
Switch> reload
Proceed with reload? [confirm] y
```

Procedure with Password Recovery Enabled

If the password-recovery mechanism 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 anything 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:
```

The switch file system appears:

```
Directory of flash:
11 -rwx 5825 Mar 01 1993 22:31:59 config.text
18 -rwx 720 Mar 01 1993 02:21:30 vlan.dat
16128000 bytes total (10003456 bytes free)
```
Step 5 Rename the configuration file to config.text.old.
   This file contains the password definition.
   
   switch: rename flash:config.text flash:config.text.old

Step 6 Boot up the system:
   
   switch: boot
   
   You are prompted to start the setup program. Enter N at the prompt:
   Continue with the configuration dialog? [yes/no]: N

Step 7 At the switch prompt, enter privileged EXEC mode:
   
   Switch> enable

Step 8 Rename the configuration file to its original name:
   
   Switch# rename flash:config.text.old flash:config.text

Step 9 Copy the configuration file into memory:
   
   Switch# copy flash:config.text system:running-config
   Source filename [config.text]?
   Destination filename [running-config]?
   
   Press Return in response to the confirmation prompts.
   
   The configuration file is now reloaded, and you can change the password.

Step 10 Enter global configuration mode:
   
   Switch# configure terminal

Step 11 Change the password:
   
   Switch (config)# enable secret password
   
   The secret password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, and allows spaces but ignores leading spaces.

Step 12 Return to privileged EXEC mode:
   
   Switch (config)# exit
   Switch#

Step 13 Write the running configuration to the startup configuration file:
   
   Switch# copy running-config startup-config
   
   The new password is now in the startup configuration.

   **Note** This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the show running-config privileged EXEC command. To re-enable the interface, enter the interface vlan vlan-id global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the no shutdown command.

Step 14 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** Elect to continue with password recovery and lose the existing configuration:

Would you like to reset the system back to the default configuration (y/n)? y

**Step 2** Load any helper files:

Switch: load_helper

**Step 3** Display the contents of flash memory:

```
switch: dir flash:
The switch file system appears:
Directory of flash:
13 drwx 192 Mar 01 1993 22:30:48 c3560-i5-mz.121.19-EA1.0
16128000 bytes total (10003456 bytes free)
```

**Step 4** 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 5** At the switch prompt, enter privileged EXEC mode:

Switch> enable

**Step 6** Enter global configuration mode:

Switch# configure terminal

**Step 7** 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 8**

Return to privileged EXEC mode:

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

**Step 9**

Write the running configuration to the startup configuration file:

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

The new password is now in the startup configuration.

---

**Note**

This procedure is likely to leave your switch virtual interface in a shutdown state. You can see which interface is in this state by entering the `show running-config` privileged EXEC command. To re-enable the interface, enter the `interface vlan vlan-id` global configuration command, and specify the VLAN ID of the shutdown interface. With the switch in interface configuration mode, enter the `no shutdown` command.

**Step 10**

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

This section describes how to recover from a failed command switch. You can configure a redundant command switch group by using the Hot Standby Router Protocol (HSRP). For more information, see Chapter 5, “Clustering Switches” and Chapter 41, “Configuring HSRP.” Also see the *Getting Started with Cisco Network Assistant*, available on Cisco.com.

**Note**

HSRP is the preferred method for supplying redundancy to a cluster.

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, page 48-8
- Replacing a Failed Command Switch with Another Switch, page 48-9

These recovery procedures require that you have physical access to the switch.

For information on command-capable switches, see the release notes.
Recovering from a Command Switch Failure

Chapter 48  Troubleshooting

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 the switch hardware installation guide.

**Step 4**  At the switch prompt, enter privileged EXEC mode:

```
Switch> enable
Switch#
```

**Step 5**  Enter the password of the failed command switch.

**Step 6**  Enter global configuration mode.

```
Switch# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 7**  Remove the member switch from the cluster.

```
Switch(config)# no cluster commander-address
```

**Step 8**  Return to privileged EXEC mode.

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

**Step 9**  Use the setup program to configure the switch IP information. This program prompts you for IP address information and passwords. From privileged EXEC mode, enter `setup`, and press Return.

```
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.

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, recall that on a command switch, the hostname is limited to 28 characters; on a member switch to 31 characters. 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, recall that it can be from 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**
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 the switch hardware installation guide.

**Step 3**
At the switch prompt, enter privileged EXEC mode:

```
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 **setup**, and press Return.

```
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.

The prompts in the setup program vary depending on the switch 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, recall that on a command switch, the hostname is limited to 28 characters. Do not use -n, where n is a number, as the last character in a hostname for any switch.

When prompted for the Telnet (virtual terminal) password, recall that it can be from 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 When 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.
Recovering from Lost Cluster Member Connectivity

Some configurations can prevent the command switch from maintaining contact with member switches. If you are unable to maintain management contact with a member, and the member switch is forwarding packets normally, check for these conflicts:

- A member switch (Catalyst 3750, Catalyst 3560, Catalyst 3550, Catalyst 3500 XL, Catalyst 2970, Catalyst 2960, Catalyst 2950, Catalyst 2900 XL, Catalyst 2820, and Catalyst 1900 switch) cannot connect to the command switch through a port that is defined as a network port.
- Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 2820, and Catalyst 1900 member switches must connect to the command switch through a port that belongs to the same management VLAN.
- A member switch (Catalyst 3750, Catalyst 3560, Catalyst 3550, Catalyst 2970, Catalyst 2960, Catalyst 2950, Catalyst 3500 XL, Catalyst 2900 XL, Catalyst 2820, and Catalyst 1900 switch) connected to the command switch through a secured port can lose connectivity if the port is disabled because of a security violation.

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 Power over Ethernet Switch Ports

These sections describe how to troubleshoot Power over Ethernet (PoE) ports.

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 is 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. 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.

Use these commands, described in the command reference for this release, to monitor the PoE port status:

- `show controllers power inline` privileged EXEC command
- `show power inline` privileged 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.

SFP Module Security and Identification

Cisco small form-factor pluggable (SFP) modules have a serial EEPROM that contains the module serial number, the vendor name and ID, a unique security code, and cyclic redundancy check (CRC). When an SFP module is inserted in the switch, the switch software reads the EEPROM to verify the serial number, vendor name and vendor ID, and recompute the security code and CRC. If the serial number, the vendor name or vendor ID, the security code, or CRC is invalid, the software generates a security error message and places the interface in an error-disabled state.

Note

The security error message references the GBIC_SECURITY facility. The switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the security messages actually refer to the SFP modules and module interfaces. For more information about error messages, see the system message guide for this release.

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 re-insert 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.

Monitoring Temperature

The Catalyst 3560G-48TS, 3560G-48PS, 3560G-24TS, and 3560G-24PS switches monitor the temperature conditions. The switch also uses the temperature information to control the fans.

Use the `show env temperature` status privileged EXEC command to display the temperature value, state, and thresholds. The temperature value is the temperature in the switch (not the external temperature). You can configure only the yellow threshold level (in Celsius) by using the `system env temperature threshold yellow value` global configuration command to set the difference between the yellow and red thresholds. You cannot configure the green or red thresholds. For more information, see the command reference for this release.

Using Ping

These sections contain this information:
- Understanding Ping, page 48-13
- Executing Ping, page 48-13

Understanding 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.

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. For more information, see Chapter 37, “Configuring IP Unicast Routing.”
IP routing is disabled by default on all switches. If you need to enable or configure IP routing, see Chapter 37, “Configuring IP Unicast Routing.”

Beginning in privileged EXEC mode, use this command to ping another device on the network from the switch:

```
ping ip host | address
```

### Purpose
Ping a remote host through IP or by supplying the hostname or network address.

**Note**

Though other protocol keywords are available with the `ping` command, they are not supported in this release.

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 Echos to 172.20.52.3, timeout is 2 seconds:

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Switch#

Table 48-1 describes the possible ping character output.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Each exclamation point means receipt of a reply.</td>
</tr>
<tr>
<td>.</td>
<td>Each period means the network server timed out while waiting for a reply.</td>
</tr>
<tr>
<td>U</td>
<td>A destination unreachable error PDU was received.</td>
</tr>
<tr>
<td>C</td>
<td>A congestion experienced packet was received.</td>
</tr>
<tr>
<td>I</td>
<td>User interrupted test.</td>
</tr>
<tr>
<td>?</td>
<td>Unknown packet type.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Packet lifetime exceeded.</td>
</tr>
</tbody>
</table>

To end a ping session, enter the escape sequence (`Ctrl-^ X by default). Simultaneously press and release the `Ctrl`, `Shift`, and `6` keys and then press the `X` key.

### Using Layer 2 Traceroute

These sections contain this information:

- Understanding Layer 2 Traceroute, page 48-15
- Usage Guidelines, page 48-15
- Displaying the Physical Path, page 48-16
Understanding 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. It finds the path by using the MAC address tables of the switches in the path. When the switch detects a device in the path that does not support Layer 2 traceroute, the switch continues to send 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.

Usage Guidelines

These are the Layer 2 traceroute usage 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.
  
  For a list of switches that support Layer 2 traceroute, see the “Usage Guidelines” section on page 48-15. If any devices in the physical path are transparent to CDP, the switch cannot identify the path through these devices. For more information about enabling CDP, see Chapter 24, “Configuring CDP.”

- A switch is reachable from another switch when you can test connectivity by using the ping privileged EXEC command. All switches 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 switches 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.

Displaying the Physical Path

You can display physical path that a packet takes from a source device to a destination device by using one of these privileged EXEC commands:

- `tracert`\`route mac [interface interface-id] {source-mac-address} [interface interface-id] {destination-mac-address} [vlan vlan-id] [detail]

- `tracert`\`route mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]

For more information, see the command reference for this release.

Using IP Traceroute

These sections contain this information:

- Understanding IP Traceroute, page 48-16
- Executing IP Traceroute, page 48-17

Understanding 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 switches can participate as the source or destination of the `tracert`\`route privileged EXEC command and might or might not appear as a hop in the `tracert`\`route command output. If the switch is the destination of the traceroute, it is displayed as the final destination in the traceroute output. Intermediate switches 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 `tracert`\`route 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.

## Executing IP Traceroute

Beginning in privileged EXEC mode, follow this step to trace that the path packets take through the network:

```bash
Switch# traceroute ip 171.9.15.10
Type escape sequence to abort.
Tracing the route to 171.9.15.10
1  172.2.52.1 0 msec 0 msec 4 msec
2  172.2.1.203 12 msec 8 msec 0 msec
3  171.9.16.6 4 msec 0 msec 0 msec
4  171.9.4.5 0 msec 4 msec 0 msec
5  171.9.121.34 0 msec 4 msec 4 msec
6  171.9.15.9 120 msec 132 msec 128 msec
7  171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

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 48-2 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>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>
</tbody>
</table>
Chapter 48  Troubleshooting

Table 48-2  Traceroute Output Display Characters (continued)

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.

Using TDR

These sections contain this information:
- Understanding TDR, page 48-18
- Running TDR and Displaying the Results, page 48-18

Understanding TDR

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 10/100 ports or 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

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. For a description of the fields in the display, see the command reference for this release.
Using Debug Commands

These sections explains how you use `debug` commands to diagnose and resolve internetworking problems:

- Enabling Debugging on a Specific Feature, page 48-19
- Enabling All-System Diagnostics, page 48-20
- Redirecting Debug and Error Message Output, page 48-20

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.

Note

For complete syntax and usage information for specific `debug` commands, see the command reference for this release.

Enabling Debugging on a Specific Feature

All `debug` commands are entered in privileged EXEC mode, and most `debug` commands take no arguments. For example, beginning in privileged EXEC mode, enter this command to enable the debugging for Switched Port Analyzer (SPAN):

```
Switch# debug span-session
```

The switch continues to generate output until you enter the `no` form of the command.

If you enable a `debug` command and no output appears, consider these possibilities:

- The switch might not be properly configured to generate the type of traffic you want to monitor. Use the `show running-config` command to check its configuration.
- Even if the switch is properly configured, it might not generate the type of traffic you want to monitor during the particular period that debugging is enabled. Depending on the feature you are debugging, you can use commands such as the TCP/IP `ping` command to generate network traffic.

To disable debugging of SPAN, enter this command in privileged EXEC mode:

```
Switch# no debug span-session
```

Alternately, in privileged EXEC mode, you can enter the `undebug` form of the command:

```
Switch# undebug span-session
```

To display the state of each debugging option, enter this command in privileged EXEC mode:

```
Switch# show debugging
```
Enabling All-System Diagnostics

Beginning in privileged EXEC mode, enter this command to enable all-system diagnostics:

```
Switch# debug all
```

**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.

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.

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.

Possible destinations include the console, virtual terminals, internal buffer, and UNIX hosts running a syslog server. The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX and its derivatives.

**Note**

Be aware that the debugging destination you use affects system overhead. Logging messages to the console produces very high overhead, whereas logging messages to a virtual terminal produces less overhead. 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 Chapter 30, “Configuring System Message Logging.”

Using the show platform forward Command

The output from the `show platform forward` privileged EXEC command provides some useful information about the forwarding results if a packet entering an interface is sent through the system. Depending upon the parameters entered about the packet, the output provides lookup table results and port maps used to calculate forwarding destinations, bitmaps, and egress information.

**Note**

For more syntax and usage information for the `show platform forward` command, see the switch command reference for this release.

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.
This is an example of the output from the `show platform forward` command on port 1 in VLAN 5 when the packet entering that port is addressed to unknown MAC addresses. The packet should be flooded to all other ports in VLAN 5.

Switch# `show platform forward gigabitethernet0/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2 udp 10 20`
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:

```
Lookup   Key-Used   Index-Hit   A-Data
InptACL 40_0D020202_0D010101-00_40000014_000A0000   01FFA   03000000
L2Local 80_00050002_00020002-00_00000000_00000000   00C71   0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005
```

Egress:ASIC 2, switch 1
Output Packets:

```
Packet 1
Lookup   Key-Used   Index-Hit   A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000   01FFE   03000000
Port  Vlan  SrcMac  DstMac  Cos  DscpV
Gi0/1  0005 0001.0001.0001  0002.0002.0002
```

Packet 2
```
Lookup   Key-Used   Index-Hit   A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000   01FFE   03000000
Port  Vlan  SrcMac  DstMac  Cos  DscpV
Gi0/2  0005 0001.0001.0001  0002.0002.0002
```

Packet dropped due to failed DEJA_VU Check on Gi1/0/2
Packet dropped due to failed DEJA_VU Check on Gi0/2

This is an example of the output when the packet coming in on port 1 in VLAN 5 is sent to an address already learned on the VLAN on another port. It should be forwarded from the port on which the address was learned.

Switch# `show platform forward gigabitethernet0/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1 13.2.2.2 udp 10 20`
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:

```
Lookup   Key-Used   Index-Hit   A-Data
InptACL 40_0D020202_0D010101-00_40000014_000A0000   01FFA   03000000
L2Local 80_00050009_43A80145-00_00000000_00000000   00086   02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003
```

Egress:ASIC 3, switch 1
Output Packets:
Using the show platform forward Command

---

Packet 1
Lookup  Key-Used  Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000 01FEE 03000000

Port  Vlan  SrcMac  DstMac  Cos  Dscp
interface-id  0005  0001.0001.0001  0009.43A8.0014

This is an example of the output when the packet coming in on port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address unknown. Because there is no default route set, the packet should be dropped.

Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 13.1.1.1 13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
Lookup  Key-Used  Index-Hit  A-Data
InptACL 40_0D020202_0D010101-00_41000014_000A0000 01FFA 03000000
L3Local 00_00000000_00000000-90_00001400_0D020202 01F0 01880290
L3Scndr 12_0D020202_0D010101-00_40000014_000A0000 034B0 000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000

This is an example of the output when the packet coming in on port 1 in VLAN 5 has a destination MAC address set to the router MAC address in VLAN 5 and the destination IP address set to an IP address that is in the IP routing table. It should be forwarded as specified in the routing table.

Switch# show platform forward gigabitethernet0/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5 16.1.10.5
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
Lookup  Key-Used  Index-Hit  A-Data
InptACL 40_10010A05_0A010505-00_41000014_000A0000 01FFA 03000000
L3Local 00_00000000_00000000-90_00001400_10010A05 01F0 01880290
L3Scndr 12_10010A05_0A010505-00_40000014_000A0000 01D28 30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

Egress:Asic 3, switch 1
Output Packets:

---

Packet 1
Lookup  Key-Used  Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000 01FEE 03000000

Port  Vlan  SrcMac  DstMac  Cos  Dscp
Gi0/2  0007 XXXX.XXXX.0246  0009.43A8.0147
Using the crashinfo Files

The crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The switch writes the crash information to the console at the time of the failure. The switch creates two types of crashinfo files:

- Basic crashinfo file—The switch automatically creates this file the next time you boot up the Cisco IOS image after the failure.
- Extended crashinfo file—The switch automatically creates this file when the system is failing.

Basic crashinfo Files

The information in the basic file includes the Cisco IOS image name and version that failed, a list of the processor registers, and other switch-specific information. You can provide this information to the Cisco technical support representative by using the `show tech-support` privileged EXEC command.

Basic crashinfo files are kept in this directory on the flash file system:

```
flash:/crashinfo/.
```

The filenames are `crashinfo_n` where `n` is a sequence number.

Each new crashinfo file that is created uses a sequence number that is larger than any previously existing sequence number, so the file with the largest sequence number describes the most recent failure. Version numbers are used instead of a timestamp because the switches do not include a real-time clock. You cannot change the name of the file that the system will use when it creates the file. However, after the file is created, you can use the `rename` privileged EXEC command to rename it, but the contents of the renamed file will not be displayed by the `show tech-support` privileged EXEC command. You can delete crashinfo files by using the `delete` privileged EXEC command.

You can display the most recent basic crashinfo file (that is, the file with the highest sequence number at the end of its filename) by entering the `show tech-support` privileged EXEC command. You also can access the file by using any command that can copy or display files, such as the `more` or the `copy` privileged EXEC command.

Extended crashinfo Files

The switch creates the extended crashinfo file when the system is failing. The information in the extended file includes additional information that can help determine the cause of the switch failure. You provide this information to the Cisco technical support representative by manually accessing the file and using the `more` or the `copy` privileged EXEC command.

Extended crashinfo files are kept in this directory on the flash file system:

```
flash:/crashinfo_ext/.
```

The filenames are `crashinfo_ext_n` where `n` is a sequence number.

You can configure the switch to not create the extended crashinfo file by using the `no exception crashinfo` global configuration command.
Memory Consistency Check Routines

The switch runs memory consistency check routines to detect and correct invalid ternary content addressable memory (TCAM) table entries that can affect the performance of the switch.

If the switch cannot fix the error, it logs a system error message, specifying the TCAM space in which the error is located:

- Unassigned space: Unassigned TCAM table entries for the current SDM template.
- Hulc Forwarding TCAM Manager (HFTM) space: Related to the Layer 2 and Layer 3 forwarding tables.
- Hulc Quality of Service (QoS)/access control list (ACL) TCAM Manager (HQATM) space: Related to ACL and ACL-like tables such as QoS classification and policy routing.

The output from the `show platform tcam errors` privileged EXEC command provides information about the TCAM memory consistency integrity on the switch.

Displaying TCAM Memory Consistency Check Errors

Beginning in privileged EXEC mode, use this command to display the TCAM memory consistency check errors detected on the switch:

```
Switch# show platform tcam errors
TCAM Memory Consistency Checker Errors
------------------------------------
TCAM Space | Values | Masks | Fixups | Retries | Failures
---------- | ------ | ------ | ------ | ------- | -------
Unassigned | 0      | 0      | 0      | 0       | 0
HFTM       | 0      | 0      | 0      | 0       | 0
HQATM      | 0      | 0      | 0      | 0       | 0
Switch#
```

This example shows information about the TCAM memory consistency integrity on the switch:

```
Switch# show platform tcam errors
TCAM Memory Consistency Checker Errors
------------------------------------
TCAM Space | Values | Masks | Fixups | Retries | Failures
---------- | ------ | ------ | ------ | ------- | -------
Unassigned | 0      | 0      | 0      | 0       | 0
HFTM       | 0      | 0      | 0      | 0       | 0
HQATM      | 0      | 0      | 0      | 0       | 0
Switch#
```

The display provides information about TCAM portions that were checked for integrity.

Table 48-3 Details of Checked TCAM Portions

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values</td>
<td>The number of invalid values found in the TCAM tables.</td>
</tr>
<tr>
<td>Masks</td>
<td>The number of invalid masks found in the TCAM tables.</td>
</tr>
<tr>
<td>Fixups</td>
<td>The number of initial attempts to fix the invalid values or masks.</td>
</tr>
<tr>
<td>Retries</td>
<td>The number of attempts to fix the invalid values or masks.</td>
</tr>
<tr>
<td>Failures</td>
<td>The number of failed attempts to fix the invalid values or masks.</td>
</tr>
</tbody>
</table>
Troubleshooting Tables

These tables are a condensed version of troubleshooting documents on Cisco.com.

- “Troubleshooting CPU Utilization” section on page 48-25
- “Troubleshooting Power over Ethernet (PoE)” section on page 48-27

Troubleshooting CPU Utilization

This section lists some possible symptoms that could be caused by the CPU being too busy and shows how to verify a CPU utilization problem. Table 48-4 lists the primary types of CPU utilization problems that you can identify. It gives possible causes and corrective action with links to the Troubleshooting High CPU Utilization document on Cisco.com.

Possible Symptoms of High CPU Utilization

Note that excessive CPU utilization might result in these symptoms, but the symptoms could 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
- BGP or OSPF routing topology changes
- HSRP flapping

Verifying the Problem and Cause

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 S5Sec M5Min T5Min 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
```
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 48-4 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>

For complete information about CPU utilization and how to troubleshoot utilization problems, see the *Troubleshooting High CPU Utilization* document on Cisco.com.
## Troubleshooting Power over Ethernet (PoE)

**Figure 48-1  Power Over Ethernet Troubleshooting Scenarios**

<table>
<thead>
<tr>
<th>Symptom or problem</th>
<th>Possible cause and solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No PoE on only one port.</td>
<td>Verify that the powered device works on another PoE port. Use the <code>show run</code>, <code>show interface status</code>, or <code>show power inline detail</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.</td>
</tr>
<tr>
<td>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 Ethernet cable from the powered device to the switch port is good: Connect a known good non-PoE Ethernet device to the Ethernet cable, and make sure that the powered device establishes a link and exchanges traffic with another host. Verify that the total cable length from the switch front panel to the powered device is not more than 100 meters. Disconnect the Ethernet cable from the switch port. Use a short Ethernet cable to connect a known good Ethernet device directly to this port on the switch front panel (not on a patch panel). Verify that it can establish an Ethernet link and exchange traffic with another host, or ping the port VLAN SVI. Next, connect a powered device to this port, and verify that it powers on. If a powered device does not power on when connected with a patch cord to the switch port, compare the total number of connected powered devices to the switch power budget (available PoE). Use the <code>show inline power</code> and <code>show inline power detail</code> commands to verify the amount of available power. For more information, see No PoE On One Port on Cisco.com.</td>
</tr>
</tbody>
</table>
## Figure 48-1 Power Over Ethernet Troubleshooting Scenarios (continued)

<table>
<thead>
<tr>
<th>Symptom or problem</th>
<th>Possible cause and solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No PoE on all ports or a group of ports. Trouble is on all switch ports. Nonpowered Ethernet devices cannot establish an Ethernet link on any port, and PoE devices do not power on.</td>
<td>If there is a continuous, intermittent, or reoccurring alarm related to power, replace the power supply if possible it is a field-replaceable unit. Otherwise, replace the switch. If the problem is on a consecutive group of ports but not all ports, the power supply is probably not defective, and the problem could be related to PoE regulators in the switch. Use the <code>show log</code> privileged EXEC command to review alarms or system messages that previously reported PoE conditions or status changes. If there are no alarms, use the <code>show interface status</code> command to verify that the ports are not shut down or error-disabled. If ports are error-disabled, use the <code>shut</code> and <code>no shut</code> interface configuration commands to re-enable the ports. Use the <code>show env power</code> and <code>show power inline</code> privileged EXEC commands to review the PoE status and power budget (available PoE). Review the running configuration to verify that <code>power inline never</code> is not configured on the ports. Connect a nonpowered Ethernet device directly to a switch port. Use only a short patch cord. Do not use the existing distribution cables. Enter the <code>shut</code> and <code>no shut</code> interface configuration commands, and verify that an Ethernet link is established. If this connection is good, use a short patch cord to connect a powered device to this port and verify that it powers on. If the device powers on, verify that all intermediate patch panels are correctly connected. Disconnect all but one of the Ethernet cables from switch ports. Using a short patch cord, connect a powered device to only one PoE port. Verify the powered device does not require more power than can be delivered by the switch port. Use the <code>show power inline</code> privileged EXEC command to verify that the powered device can receive power when the port is not shut down. Alternatively, watch the powered device to verify that it powers on. If a powered device can power on when only one powered device is connected to the switch, enter the <code>shut</code> and <code>no shut</code> interface configuration commands on the remaining ports, and then reconnect the Ethernet cables one at a time to the switch PoE ports. Use the <code>show interface status</code> and <code>show power inline</code> privileged EXEC commands to monitor inline power statistics and port status. If there is still no PoE at any port, a fuse might be open in the PoE section of the power supply. This normally produces an alarm. Check the log again for alarms reported earlier by system messages. For more information, see No PoE On Any Port or a Group of Ports on Cisco.com.</td>
</tr>
</tbody>
</table>
Cisco IP Phone disconnects or resets. After working normally, a Cisco phone or wireless access point intermittently reloads or disconnects from PoE.

- Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads.
- Verify that the cable length is not more than 100 meters from the switch port to the powered device.
- Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs?
- Notice whether any error messages appear at the same time a disconnect occurs. Use the `show log` privileged EXEC command to review error messages.
- Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.)
- Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device.

For more information, see Cisco Phone Disconnects or Resets on Cisco.com.

Non-Cisco powered device does not work on Cisco PoE switch. A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.

- Use the `show power inline` command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected.
- Verify that sufficient power is available for the powered device type before you connect it.
- Use the `show interface status` command to verify that the switch detects the connected powered device.
- Use the `show log` command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or inrush) current that exceeds a current-limit threshold for the port.

For more information, see Non-Cisco PD Does Not Work Correctly on Cisco PoE Switch on Cisco.com.

<table>
<thead>
<tr>
<th>Symptom or problem</th>
<th>Possible cause and solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Phone disconnects or resets. After working normally, a Cisco phone or wireless access point intermittently reloads or disconnects from PoE.</td>
<td>Verify all electrical connections from the switch to the powered device. Any unreliable connection results in power interruptions and irregular powered device functioning such as erratic powered device disconnects and reloads. Verify that the cable length is not more than 100 meters from the switch port to the powered device. Notice what changes in the electrical environment at the switch location or what happens at the powered device when the disconnect occurs? Notice whether any error messages appear at the same time a disconnect occurs. Use the <code>show log</code> privileged EXEC command to review error messages. Verify that an IP phone is not losing access to the Call Manager immediately before the reload occurs. (It might be a network problem and not a PoE problem.) Replace the powered device with a non-PoE device, and verify that the device works correctly. If a non-PoE device has link problems or a high error rate, the problem might be an unreliable cable connection between the switch port and the powered device. For more information, see Cisco Phone Disconnects or Resets on Cisco.com.</td>
</tr>
<tr>
<td>Non-Cisco powered device does not work on Cisco PoE switch. A non-Cisco powered device is connected to a Cisco PoE switch, but never powers on or powers on and then quickly powers off. Non-PoE devices work normally.</td>
<td>Use the <code>show power inline</code> command to verify that the switch power budget (available PoE) is not depleted before or after the powered device is connected. Verify that sufficient power is available for the powered device type before you connect it. Use the <code>show interface status</code> command to verify that the switch detects the connected powered device. Use the <code>show log</code> command to review system messages that reported an overcurrent condition on the port. Identify the symptom precisely: Does the powered device initially power on, but then disconnect? If so, the problem might be an initial surge-in (or inrush) current that exceeds a current-limit threshold for the port. For more information, see Non-Cisco PD Does Not Work Correctly on Cisco PoE Switch on Cisco.com.</td>
</tr>
</tbody>
</table>
Configuring Online Diagnostics

This chapter describes how to configure the online diagnostics on the Catalyst 3560 switches.

For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release.

This chapter consists of these sections:

- Understanding How Online Diagnostics Work, page 49-1
- Running Online Diagnostic Tests, page 49-3

Understanding How Online Diagnostics Work

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.
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 specific switch. Use the `no` form of this command to remove the scheduling.

Beginning in global configuration mode, use this command to schedule online diagnostics:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diagnostic schedule test</code></td>
<td>Schedule on-demand diagnostic tests for a specific date and time, how many times to run the test (iterations), and what action to take when errors are found.</td>
</tr>
<tr>
<td><code>diagnostic monitor interval test</code></td>
<td>Configure the health-monitoring interval of the specified tests. By default, monitoring is disabled.</td>
</tr>
<tr>
<td><code>diagnostic monitor syslog</code></td>
<td>Enable the generation of a syslog message for health-monitoring test failures. By default, syslog is disabled.</td>
</tr>
<tr>
<td><code>diagnostic monitor threshold test</code></td>
<td>Set the failure threshold for monitoring tests. By default, monitoring is disabled.</td>
</tr>
</tbody>
</table>

This example shows how to schedule diagnostic testing on a specific date and time for a specific switch:

```
Switch(config)# diagnostic schedule test 1,2,4-6 on january 3 2006 23:32
```

This example shows how to schedule diagnostic testing to occur weekly at a certain time for a specific switch:

```
Switch(config)# diagnostic schedule test 1,2,4-6 weekly friday 09:23
```

Configuring Health-Monitoring Diagnostics

You can configure health-monitoring diagnostic testing while the switch is connected to a live network. You can configure the execution interval for each health-monitoring test, whether or not to generate a system message upon a test failure, or to enable or disable an individual test. Use the `no` form of this command to disable testing.

Beginning in global configuration mode, use these commands to configure health-monitoring diagnostics:

Use the `no diagnostic monitor interval test` 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` command to remove the failure threshold.
This example shows how to configure the specified test to run every 2 minutes:

```
Switch(config)# diagnostic monitor interval test 1 00:02:00 0 1
```

This example shows how to set the failure threshold for test monitoring on a switch:

```
Switch(config)# diagnostic monitor threshold test 1 failure count 50
```

This example shows how to enable the generation of a syslog message when any health monitoring test fails:

```
Switch(config)# diagnostic monitor syslog
```

## Running Online Diagnostic Tests

After you configure online diagnostics, you can start diagnostic tests or display the test results. You can also see which tests are configured for each switch and what diagnostic tests have already run.

These sections describe how to run online diagnostic tests after they have been configured:

- Starting Online Diagnostic Tests, page 49-3
- Displaying Online Diagnostic Tests and Test Results, page 49-4

### Starting Online Diagnostic Tests

After you configure diagnostic tests to run on the switch or on individual switches, you can use `start` to begin a diagnostic test.

Beginning in global configuration mode, use this command to start an online diagnostic test:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>diagnostic start test</strong> test-id</td>
<td>Start a diagnostic test on a specific switch.</td>
</tr>
<tr>
<td><strong>diagnostic start test</strong> test-id-range</td>
<td></td>
</tr>
<tr>
<td><strong>diagnostic start test</strong> all</td>
<td></td>
</tr>
<tr>
<td><strong>diagnostic start test</strong> basic</td>
<td></td>
</tr>
<tr>
<td><strong>diagnostic start test</strong> non-disruptive</td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to start a diagnostic test on a specific switch:

```
Switch# diagnostic start test 1
Switch# 06:27:50: %DIAG-6-TEST_RUNNING: Running TestPortAsicStackPortLoopback(ID=1) ...
Switch# 06:27:51: %DIAG-6-TEST_OK: TestPortAsicStackPortLoopback(ID=1) has completed successfully
```

Displaying Online Diagnostic Tests and Test Results

You can display the online diagnostic tests that are configured for specific switches and check the results of the tests using the `show` commands.

To display the diagnostic tests that are configured for a switch and the test results, use these privileged EXEC commands:

```
Table 49-1   show diagnostic Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show diagnostic content</td>
<td>Display the online diagnostics configured for a switch.</td>
</tr>
<tr>
<td>show diagnostic status</td>
<td>Display whether a switch is running a test.</td>
</tr>
<tr>
<td>show diagnostic result</td>
<td>Display the online diagnostics test results.</td>
</tr>
<tr>
<td></td>
<td>test [test_id \ test_id_range [detail]]</td>
</tr>
<tr>
<td>show diagnostic schedule</td>
<td>Display the online diagnostics test schedule.</td>
</tr>
<tr>
<td>show diagnostic post</td>
<td>Display the results of POST. (The same as the show post command.)</td>
</tr>
</tbody>
</table>
```

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 on demand 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

ID Test Name attributes Test Interval Threshold
== =============== =================== ===========
1) TestPortAsicStackPortLoopback B*N****A** 000 00:01:00.00 n/a
2) TestPortAsicLoopback B*D*X**IR* not configured n/a
3) TestPortAsicCam B*D*X**IR* not configured n/a
4) TestPortAsicRingLoopback B*D*X**IR* not configured n/a
5) TestMicRingLoopback B*D*X**IR* not configured n/a
6) TestPortAsicMem B*D*X**IR* not configured n/a
```

This example shows how to display the online diagnostic results for a switch:

```
Switch# show diagnostic result
Overall diagnostic result: PASS
Test results: (. = Pass, F = Fail, U = Untested)
1) TestPortAsicStackPortLoopback --> .
2) TestPortAsicLoopback ---------- .
3) TestPortAsicCam -------------- .
4) TestPortAsicRingLoopback ------ .
5) TestMicRingLoopback ---------- .
6) TestPortAsicMem -------------- .
```

This example shows how to display the online diagnostic test schedule for a switch:
Switch# `show diagnostic schedule`
Current Time = 14:39:49 PST Tue Jul 5 2005
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
Supported MIBs

This appendix lists the supported management information base (MIBs) for this release on the Catalyst 3560 switch. It contains these sections:

- **MIB List, page A-1**
- **Using FTP to Access the MIB Files, page A-4**

### MIB List

- **BRIDGE-MIB**
  
  **Note** The BRIDGE-MIB supports the context of a single VLAN. By default, SNMP messages using the configured community string always provide information for VLAN 1. To obtain the BRIDGE-MIB information for other VLANs, for example VLAN x, use this community string in the SNMP message: configured community string @x.

- **CISCO-ADMISSION-POLICY-MIB**
- **CISCO-AUTH-FRAMEWORK-MIB**
- **CISCO-CABLE-DIAG-MIB**
- **CISCO-CDP-MIB**
- **CISCO-CLUSTER-MIB**
- **CISCO-CONFIG-COPY-MIB**
- **CISCO-CONFIG-MAN-MIB**
- **CISCO-ENTITY-FRU-CONTROL-MIB**
- **CISCO-ENTITY-VENDORTYPE-OID-MIB**
- **CISCO-ENVMON-MIB**
- **CISCO-ERR-DISABLE-MIB**
- **CISCO-FLASH-MIB** (Flash memory on all switches is modeled as removable flash memory.)
- **CISCO-FTP-CLIENT-MIB**
- **CISCO-HSRP-MIB**
- **CISCO-HSRP-EXT-MIB** (partial support)
• CISCO-IETF-IP-MIB
• CISCO-IETF-IP-FORWARDING-MIB
• CISCO-IGMP-FILTER-MIB
• CISCO-IMAGE-MIB
• CISCO IP-STAT-MIB
• CISCO-L2L3-INTERFACE-CONFIG-MIB
• CISCO-LAG-MIB
• CISCO-MAC-AUTH-BYPASS
• CISCO-MAC-NOTIFICATION-MIB
• CISCO-MEMORY-POOL-MIB
• CISCO-NAC-NAD-MIB
• CISCO-PAE-MIB
• CISCO-PAGP-MIB
• CISCO-PING-MIB
• CISCO-PORT-QOS-MIB (only the packet counters are supported; the octet counters are not supported)
• CISCO-POWER-ETHERNET-EXT-MIB
• CISCO-PRODUCTS-MIB
• CISCO-PROCESS-MIB
• CISCO-RTTMON-MIB
• CISCO-SMI-MIB
• CISCO-STP-EXTENSIONS-MIB
• CISCO-SYSLOG-MIB
• CISCO-TC-MIB
• CISCO-TCP-MIB
• CISCO-UDLD-MIB
• CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
• CISCO-VLAN-MEMBERSHIP-MIB
• CISCO-VTP-MIB
• CISCO-CONFIG-COPY-MIB
• ENTITY-MIB
• ETHERLIKE-MIB
• IEEE8021-PAE-MIB
• IEEE8023-LAG-MIB
• IF-MIB (In and out counters for VLANs are not supported.)
• IGMP-MIB
• INET-ADDRESS-MIB
• IPMROUTE-MIB
• LLDP MED MIB
• OLD-CISCO-CHASSIS-MIB
• OLD-CISCO-FLASH-MIB
• OLD-CISCO-INTERFACES-MIB
• OLD-CISCO-IP-MIB
• OLD-CISCO-SYS-MIB
• OLD-CISCO-TCP-MIB
• OLD-CISCO-TS-MIB
• PIM-MIB
• RFC1213-MIB (Functionality is as per the agent capabilities specified in the CISCO-RFC1213-CAPABILITY.my.)
• RFC1253-MIB (OSPF-MIB)
• RMON-MIB
• RMON2-MIB
• SNMP-FRAMEWORK-MIB
• SNMP-MPD-MIB
• SNMP-NOTIFICATION-MIB
• SNMP-TARGET-MIB
• SNMPv2-MIB
• TCP-MIB
• UDP-MIB

---

**Note**

You can also use this URL for a list of supported MIBs for the Catalyst 3560 switch:

You can access other information about MIBs and Cisco products on the Cisco web site:
Using FTP to Access the MIB Files

You can get each MIB file by using this procedure:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Make sure that your FTP client is in passive mode.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Some FTP clients do not support passive mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Use FTP to access the server ftp.cisco.com.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Log in with the username anonymous.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter your e-mail username when prompted for the password.</td>
</tr>
<tr>
<td>Step 5</td>
<td>At the ftp&gt; prompt, change directories to /pub/mibs/v1 and /pub/mibs/v2.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Use the get MIB_filename command to obtain a copy of the MIB file.</td>
</tr>
</tbody>
</table>
Working with the Cisco IOS File System, Configuration Files, and Software Images

This appendix describes how to manipulate the Catalyst 3560 switch flash file system, how to copy configuration files, and how to archive (upload and download) software images to a switch.

Note
For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 from the Cisco.com page under Documentation > Cisco IOS Software > 12.2 Mainline > Command References.

This appendix has these sections:
- Working with the Flash File System, page B-1
- Working with Configuration Files, page B-8
- Working with Software Images, page B-24

Working with 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 image and configuration files. The default flash file system on the switch is named flash:

These sections contain this configuration information:
- Displaying Available File Systems, page B-2
- , page B-2
- Displaying Information about Files on a File System, page B-3
- Creating and Removing Directories, page B-4
- Copying Files, page B-4
- Deleting Files, page B-5
- Creating, Displaying, and Extracting tar Files, page B-5
- Displaying the Contents of a File, page B-7
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.

Switch# show file systems

<table>
<thead>
<tr>
<th>File Systems:</th>
<th>Size(b)</th>
<th>Free(b)</th>
<th>Type</th>
<th>Flags</th>
<th>Prefixes</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 15998976</td>
<td>5135872</td>
<td>flash</td>
<td>rw</td>
<td>flash:flash3:</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>bs:</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>vb:</td>
<td></td>
</tr>
<tr>
<td>524288</td>
<td>520138</td>
<td>nvram</td>
<td>rw</td>
<td>nvram:</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>network</td>
<td>rw</td>
<td>tftp:</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>null:</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>rw</td>
<td>system:</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>ro</td>
<td>xmodem:</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>opaque</td>
<td>ro</td>
<td>ymodem:</td>
<td></td>
</tr>
</tbody>
</table>

Table B-1 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>flash—The file system is for a flash memory device.</td>
</tr>
<tr>
<td></td>
<td>nvram—The file system is for a NVRAM device.</td>
</tr>
<tr>
<td></td>
<td>opaque—The file system is a locally generated pseudo file system (for example, the system) or a download interface, such as brimux.</td>
</tr>
<tr>
<td></td>
<td>unknown—The file system is an unknown type.</td>
</tr>
<tr>
<td>Flags</td>
<td>Permission for file system.</td>
</tr>
<tr>
<td></td>
<td>ro—read-only.</td>
</tr>
<tr>
<td></td>
<td>rw—read/write.</td>
</tr>
<tr>
<td></td>
<td>wo—write-only.</td>
</tr>
<tr>
<td>Prefixes</td>
<td>Alias for file system.</td>
</tr>
<tr>
<td></td>
<td>flash:—Flash file system.</td>
</tr>
<tr>
<td></td>
<td>nvram:—NVRAM.</td>
</tr>
<tr>
<td></td>
<td>null:—Null destination for copies. You can copy a remote file to null to find its size.</td>
</tr>
<tr>
<td></td>
<td>rcp:—Remote Copy Protocol (RCP) network server.</td>
</tr>
<tr>
<td></td>
<td>system:—Contains the system memory, including the running configuration.</td>
</tr>
<tr>
<td></td>
<td>tftp:—TFTP network server.</td>
</tr>
<tr>
<td></td>
<td>xmodem:—Obtain the file from a network machine by using the Xmodem protocol.</td>
</tr>
<tr>
<td></td>
<td>ymodem:—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 in Table B-2:

<table>
<thead>
<tr>
<th>Table B-2</th>
<th>Commands for Displaying Information About Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>dir [/all] [filesystem:][filename]</td>
<td>Display a list of files on a file system.</td>
</tr>
<tr>
<td>show file systems</td>
<td>Display more information about each of the files on a file system.</td>
</tr>
<tr>
<td>show file information file-url</td>
<td>Display information about a specific file.</td>
</tr>
<tr>
<td>show file descriptors</td>
<td>Display 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>

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dir filesystem:</td>
<td>Display the directories on the specified file system. For <code>filesystem:</code>; use <code>flash:</code> for the system board flash device.</td>
</tr>
<tr>
<td>2</td>
<td>cd new_configs</td>
<td>Change to the directory of interest. The command example shows how to change to the directory named <code>new_configs</code>.</td>
</tr>
<tr>
<td>3</td>
<td>pwd</td>
<td>Display the working directory.</td>
</tr>
</tbody>
</table>
# Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create and remove a directory:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>dir filesystem:</strong> Display the directories on the specified file system.</td>
</tr>
<tr>
<td></td>
<td><strong>For filesystem:</strong> use flash: for the system board flash device.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>mkdir old_configs</strong> Create a new directory.</td>
</tr>
<tr>
<td></td>
<td><strong>The command example shows how to create the directory named old_configs.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Directory names are case sensitive.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>dir filesystem:</strong> Verify your entry.</td>
</tr>
</tbody>
</table>

To delete 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. 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.

For `filesystem`, use `flash:` for the system board flash device. For `file-url`, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

⚠️ **Caution**

When files and directories are deleted, their contents cannot be recovered.

# Copying Files

To copy a file from a source to a destination, use the `copy source-url destination-url` privileged EXEC command. For the source and destination URLs, you can use `running-config` and `startup-config` keyword shortcuts. For example, the `copy running-config startup-config` command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special 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)

For specific examples of using the `copy` command with configuration files, see the “Working with Configuration Files” section on page B-8.

To copy software images either by downloading a new version or by uploading the existing one, use the `archive download-sw` or the `archive upload-sw` privileged EXEC command. For more information, see the “Working with Software Images” section on page B-24.

### Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the `delete [force] [recursive] filesystem:/file-url` privileged EXEC command.

Use the `/recursive` keyword for deleting a directory and all subdirectories and the files contained in it. Use the `/force` keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the `/force` and `/recursive` keywords for deleting old software images that were installed by using the `archive download-sw` command but are no longer needed.

If you omit the `filesystem:` option, the switch uses the default device specified by the `cd` command. For `file-url`, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.

---

**Caution**
When files are deleted, their contents cannot be recovered.

This example shows how to delete the file `myconfig` from the default flash memory device:

```
Switch# delete myconfig
```

### Creating, Displaying, and Extracting tar Files

You can create a tar file and write files into it, list the files in a tar file, and extract the files from a tar file as described in the next sections.

---

**Note**
Instead of using the `copy` privileged EXEC command or the `archive tar` privileged EXEC command, we recommend using the `archive download-sw` and `archive upload-sw` privileged EXEC commands to download and upload software image files.
Creating a tar File

To create a tar file and write files into it, use this privileged EXEC command:

```
archive tar /create destination-url flash:/file-url
```

For `destination-url`, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- For the local flash file system, the syntax is `flash:`
- For the FTP, the syntax is `ftp://[[username:[password]@location]/directory]/tar-filename.tar`
- For the RCP, the syntax is `rcp://[[username@location]/directory]/tar-filename.tar`
- For the TFTP, the syntax is `tftp://[[location]/directory]/tar-filename.tar`

The `tar-filename.tar` is the tar file to be created.

For `flash:/file-url`, specify the location on the local flash file system from which the new tar file is created. You can also specify an optional list of files or directories within the source directory to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

This example shows how to create a tar file. This command writes the contents of the `new-configs` directory on the local flash device to a file named `saved.tar` on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a tar File

To display the contents of a tar file on the screen, use this privileged EXEC command:

```
archive tar /table source-url
```

For `source-url`, specify the source URL alias for the local or network file system. These options are supported:

- For the local flash file system, the syntax is `flash:`
- For the FTP, the syntax is `ftp://[[username:[password]@location]/directory]/tar-filename.tar`
- For the RCP, the syntax is `rcp://[[username@location]/directory]/tar-filename.tar`
- For the TFTP, the syntax is `tftp://[[location]/directory]/tar-filename.tar`

The `tar-filename.tar` is the tar file to display.

You can also limit the display of the files by specifying an optional list of files or directories after the tar file; then only those files appear. If none are specified, all files and directories appear.

This example shows how to display the contents of a switch tar file that is in flash memory:

```
Switch# archive tar /table flash:image-name.tar
image-name/ (directory)
image-name/html/ (directory)
image-name/html/foo.html (0 bytes)
```
image-name/image-name.bin (610856 bytes)
image-name/info (219 bytes)

This example shows how to display only the /html directory and its contents:

Switch# archive tar /table flash: image-name/html
cimage-name/html
cimage-name/html/ (directory)
cimage-name/html/const.htm (556 bytes)
cimage-name/html/xhome.htm (9373 bytes)
cimage-name/html/menu.css (1654 bytes)
<output truncated>

### Extracting a tar File

To extract a tar file into a directory on the flash file system, use this privileged EXEC command:

```
archive tar /xtract source-url flash:/file-url [dir/file...]
```

For `source-url`, specify the source URL alias for the local file system. These options are supported:

- For the local flash file system, the syntax is
  `flash:`
- For the FTP, the syntax is
  `ftp:[[username][:password]@location][directory]/tar-filename.tar`
- For the RCP, the syntax is
  `rcp:[[username@location][directory]/tar-filename.tar`
- For the TFTP, the syntax is
  `tftp:[[location][directory]/tar-filename.tar`

The `tar-filename.tar` is the tar file from which to extract files.

For `flash:/file-url [dir/file...]`, specify the location on the local flash file system into which the tar file is extracted. Use the `dir/file...` option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.

This example shows how to extract the contents of a tar file located on the TFTP server at 172.20.10.30. This command extracts just the `new-configs` directory into the root directory on the local flash file system. The remaining files in the `saved.tar` file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

### Displaying the Contents of a File

To display the contents of any readable file, including a file on a remote file system, use the `more` `/ascii | /binary | /ebcdic` `file-url` privileged EXEC command:

This example shows how to display the contents of a configuration file on a TFTP server:

```
Switch# more tftp://serverA/hampton/savedconfig
! Saved configuration on server
! version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
! <output truncated>
```
Working with Configuration Files

This section describes how to create, load, and maintain 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. For more information, see Chapter 3, “Assigning the Switch IP Address and Default Gateway.”

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.

These sections contain this configuration information:

- Guidelines for Creating and Using Configuration Files, page B-9
- Configuration File Types and Location n, page B-9
- Creating a Configuration File By Using a Text Editor, page B-10
- Copying Configuration Files By Using TFTP, page B-10
- Copying Configuration Files By Using FTP, page B-12
- Copying Configuration Files By Using RCP, page B-16
- Clearing Configuration Information, page B-19
- Replacing and Rolling Back Configurations, page B-19
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 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, 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.

Note

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:

**Step 1** Copy an existing configuration from a switch to a server.

For more information, see the “Downloading the Configuration File By Using TFTP” section on page B-11, the “Downloading a Configuration File By Using FTP” section on page B-13, or the “Downloading a Configuration File By Using RCP” section on page B-17.

**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.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using TFTP, page B-10
- Downloading the Configuration File By Using TFTP, page B-11
- Uploading the Configuration File By Using TFTP, page B-12

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:

---

**Step 1**  
Copy the configuration file to the appropriate TFTP directory on the workstation.

**Step 2**  
Verify that the TFTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using TFTP” section on page B-10.

**Step 3**  
Log into the switch through the console 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`
- `copy tftp://[[location]/directory]/filename nvram:startup-config`

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.

---

This example shows how to configure the software from the file *tokyo-confg* at IP address 172.16.2.155:

```
Switch# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```
Uploading the Configuration File By Using TFTP

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

---

**Step 1** Verify that the TFTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using TFTP” section on page B-10.

**Step 2** Log into the switch through the console 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]`

The file is uploaded to the TFTP server.

---

This example shows how to upload a configuration file from a switch to a TFTP server:

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
Writing tokyo-config!!! [OK]
```

Copying Configuration Files By Using FTP

You can copy configuration 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 a configuration 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 `copy` 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 `copy` 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 your FTP write request.

Use the `ip ftp username` and `ip ftp password` commands to specify a username and password for all copies. Include the username in the `copy` command if you want to specify only a username for that copy operation.
If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user's name as the remote username.

For more information, see the documentation for your FTP server.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using FTP, page B-13
- Downloading a Configuration File By Using FTP, page B-13
- Uploading a Configuration File By Using FTP, page B-15

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using FTP” section on page B-13.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3 <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 4, 5, and 6).</td>
</tr>
<tr>
<td>Step 4 <code>ip ftp username username</code></td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 5 <code>ip ftp password password</code></td>
<td>(Optional) Change the default password.</td>
</tr>
</tbody>
</table>
### Working with Configuration Files

**Working with Configuration Files**

This example shows how to copy a configuration file named `host1-config` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
```

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
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
```

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>copy ftp://username:password@location/directory/filename</code> system:running-config</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>or</td>
<td></td>
</tr>
<tr>
<td><code>copy ftp://username:password@location/directory/filename nvram:startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>

This example shows how to copy a configuration file named `host1-config` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
```

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
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
```

Switch# %SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from 172.16.101.101

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Step 7</strong></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>copy ftp://username:password@location/directory/filename</code> system:running-config</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>or</td>
<td></td>
</tr>
<tr>
<td><code>copy ftp://username:password@location/directory/filename nvram:startup-config</code></td>
<td></td>
</tr>
</tbody>
</table>
Uploading a Configuration File By Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using FTP” section on page B-13.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Log into the switch through the console port or a Telnet session.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enter global configuration mode.</strong> This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).</td>
<td></td>
</tr>
<tr>
<td><strong>(Optional) Change the default remote username.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>(Optional) Change the default password.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Return to privileged EXEC mode.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Using FTP, store the switch running or startup configuration file to the specified location.</strong></td>
<td></td>
</tr>
</tbody>
</table>

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 ftp://netadmin1:mypass@172.16.101.101/switch2-confg
Write file switch2-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 by using FTP to copy the file:

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[?] 172.16.101.101
Name of configuration file to write [switch2-confg]?
Write file switch2-confg on host 172.16.101.101?[confirm]
! [OK]
```
Copying Configuration Files By Using RCP

The RCP provides another method of downloading, uploading, and copying configuration files between remote hosts and the switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the switch to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the `copy` command if a username is specified.
- The username set by the `ip rcmd remote-username username` global configuration command if the command is configured.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the `username` command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

These sections contain this configuration information:

- Preparing to Download or Upload a Configuration File By Using RCP, page B-16
- Downloading a Configuration File By Using RCP, page B-17
- Uploading a Configuration File By Using RCP, page B-18

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 subnet 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using RCP” section on page B-16.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><em>configure terminal</em></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Specify the remote username.</td>
</tr>
<tr>
<td><em>ip rcmd remote-username</em></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><em>username</em></td>
<td>Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
</tbody>
</table>

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]
%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-confg` from the `netadmin1` directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```plaintext
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[rt2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:[OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from 172.16.101.101
```

### Uploading a Configuration File By Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using RCP” section on page B-16.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>This step is required only if you override the default remote username (see Steps 4 and 5).</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>ip rcmd remote-username username</code></td>
</tr>
<tr>
<td></td>
<td><em>(Optional)</em> Specify the remote username.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>copy system:running-config rcp:(/[username@]location[/directory]/filename]</code></td>
</tr>
<tr>
<td>or <code>copy nvram:startup-config rcp:(/[username@]location[/directory]/filename]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Using RCP, copy the configuration file from a switch running or startup configuration file to a network server.</td>
</tr>
</tbody>
</table>

This example shows how to copy the running configuration file named `switch2-config` to the `netadmin1` directory on the remote host with an IP address of 172.16.101.101:

```plaintext
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-config
Write file switch-conf 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-config]? switch2-config
Write file switch2-config on host 172.16.101.101?[confirm] ![OK]
```

### 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.

⚠️ **Caution**

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 12.2*.

⚠️ **Caution**

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. These sections contain this information:

- Understanding Configuration Replacement and Rollback, page B-20
- Configuration Guidelines, page B-21
- Configuring the Configuration Archive, page B-22
- Performing a Configuration Replacement or Rollback Operation, page B-23
Understanding Configuration Replacement and Rollback

To use the configuration replacement and rollback feature, you should understand these concepts:
- Archiving a Configuration, page B-20
- Replacing a Configuration, page B-20
- Rolling Back a Configuration, page B-21

Archiving a Configuration

The configuration archive provides a mechanism to store, organize, and manage an archive of configuration files. The `configure replace` privileged EXEC command increases the configuration rollback capability. As an alternative, you can save copies of the running configuration by using the `copy running-config destination-url` privileged EXEC command, storing the replacement file either locally or remotely. However, this method lacks any automated file management. The configuration replacement and rollback feature can automatically save copies of the running configuration to the configuration archive.

You use the `archive config` privileged EXEC command to save configurations in the configuration archive by 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. You can specify how many versions of the running configuration are kept in the archive. After the maximum number of files are saved, the oldest file is automatically deleted when the next, most recent file is saved. The `show archive` privileged EXEC command displays information for all the configuration files saved in the configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the `configure replace` command, is in any of these file systems: FTP, HTTP, RCP, TFTP.

Replacing a Configuration

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.
Rolling Back a Configuration

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:

<table>
<thead>
<tr>
<th>Command</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>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>archive</code></td>
<td>Enter archive configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>path url</code></td>
<td>Specify the location and filename prefix for the files in the configuration archive.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>maximum number</code></td>
<td>(Optional) Set the maximum number of archive files of the running configuration to be saved in the configuration archive.</td>
</tr>
<tr>
<td><code>number</code>—Maximum files of the running configuration file in the configuration archive. Valid values are from 1 to 14. The default is 10.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Before using this command, you must first enter the <code>path archive configuration</code> command to specify the location and filename prefix for the files in the configuration archive.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>time-period minutes</code></td>
<td>(Optional) Set the time increment for automatically saving an archive file of the running configuration in the configuration archive.</td>
</tr>
<tr>
<td><code>minutes</code>—Specify how often, in minutes, to automatically save an archive file of the running configuration in the configuration archive.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>archive config</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>configure replace <code>target-url [list] [force] [time seconds] [nolock]</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>configure confirm</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>
Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, the Cisco IOS code, and the embedded device manager software.

Note

Instead of using the copy privileged EXEC command or the archive tar privileged EXEC command, we recommend using the archive download-sw and archive upload-sw privileged EXEC commands to download and upload software image files.

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 can use the archive download-sw /allow-feature-upgrade privileged EXEC command to allow installation of an image with a different feature set, for example, upgrading from the IP base image to the IP services image. Beginning in this release, you can also use the boot auto-download-sw global configuration command to specify a URL to use to get an image for automatic software upgrades.

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.

These sections contain this configuration information:

- Image Location on the Switch, page B-25
- tar File Format of Images on a Server or Cisco.com, page B-25
- Copying Image Files By Using TFTP, page B-26
- Copying Image Files By Using FTP, page B-29
- Copying Image Files By Using RCP, page B-34

Note

For a list of software images and the supported upgrade paths, see the release notes.
Image Location on the Switch

The Cisco IOS image is stored as a .bin file in a directory that shows the version number. A subdirectory contains the files needed for web management. The image is stored on the system board flash memory (flash:).

You can use the `show version` privileged EXEC command to see the software version that is currently running on your switch. In the display, check the line that begins with `System image file is...`. It shows the directory name in flash memory where the image is stored.

You can also use the `dir filesystem:` privileged EXEC command to see the directory names of other software images that might be stored in flash memory. The `archive download-sw /directory` privileged EXEC command allows you to specify a directory one time followed by a tar file or list of tar files to be downloaded instead of specifying complete paths with each tar file.

tar 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. Table B-3 provides additional details about this information:

```
system_type:0x00000000:image-name
  image_family:xxxx
  stacking_number:x
  info_end:
version_suffix:xxxx
  version_directory:image-name
  image_system_type_id:0x00000000
  image_name:image-nameB.bin
  ios_image_file_size:6398464
  total_image_file_size:8133632
  image_feature:IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
  image_family:xxxx
  stacking_number:x
  board_ids:0x401100c4 0x00000000 0x00000001 0x00000003 0x00000002 0x00008000 0x00008002 0x40110000
  info_end:
```

Note: Disregard the `stacking_number` field. It does not apply to the switch.

<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>
</tbody>
</table>
Copying Image Files By 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.

These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using TFTP, page B-26
- Downloading an Image File By Using TFTP, page B-27
- Uploading an Image File By Using TFTP, page B-29

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

---

**Note**  You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a `fastboot` command (on the SunOS 4.x) or a `reboot` command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

---

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnet if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the `ping` command.
- Ensure that the 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Copy the image to the appropriate TFTP directory on the workstation. Make sure that the TFTP server is properly configured; see the “Preparing to Download or Upload an Image File By Using TFTP” section on page B-26.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
</tbody>
</table>
### Working with Software Images

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 3**<br>archive download-sw /allow-feature-upgrade /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 `/allow-feature-upgrade` option allows installation of an image with a different feature set.  
- 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<br>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**<br>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 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 image. All the files in the directory and the directory are removed.
### Caution
For the download and upload algorithms to operate properly, do not rename image names.

### Uploading an Image File By 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Make sure the TFTP server is properly configured; see the &quot;Preparing to Download or Upload an Image File By Using TFTP&quot; section on page B-26.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td><strong>Step 3</strong> archive upload-sw</td>
<td>Upload the currently running switch image to the TFTP server.</td>
</tr>
<tr>
<td>tftp://[//location]/directory/image-name.tar</td>
<td>• For //location, specify the IP address of the TFTP server.</td>
</tr>
<tr>
<td></td>
<td>• For /directory/image-name.tar, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The image-name.tar is the name of the software image to be stored on the server.</td>
</tr>
</tbody>
</table>

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.

### Caution
For the download and upload algorithms to operate properly, do not rename image names.

### Copying Image Files By Using FTP

You can download a switch image from an FTP server or upload the image from the switch to an FTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the switch or another switch of the same type.

### Note
Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files.
These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using FTP, page B-30
- Downloading an Image File By Using FTP, page B-31
- Uploading an Image File By Using FTP, page B-33

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` 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` 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Verify that the FTP server is properly</td>
<td>Verify that the FTP server is properly configured by referring to the</td>
</tr>
<tr>
<td>configured by referring to the “Preparing to</td>
<td>“Preparing to Download or Upload an Image File By Using FTP” section</td>
</tr>
<tr>
<td>Download or Upload an Image File By Using FTP”</td>
<td>on page B-30.</td>
</tr>
<tr>
<td>Step 2 Log into the switch through the console</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>port or a Telnet session.</td>
<td></td>
</tr>
<tr>
<td>Step 3 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 4 ip ftp username <em>username</em></td>
<td>(Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 5 ip ftp password <em>password</em></td>
<td>(Optional) Change the default password.</td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 archive download-sw /allow-feature-upgrade</td>
<td>Download the image file from the FTP server to the switch, and</td>
</tr>
<tr>
<td>/overwrite /reload</td>
<td>overwrite the current image.</td>
</tr>
<tr>
<td>ftp://[//username[:password]@location]/directory</td>
<td>• The <strong>/allow-feature-upgrade</strong> option allows installation of an image with a different feature set.</td>
</tr>
<tr>
<td>/image-name.tar</td>
<td>• The <strong>/overwrite</strong> option overwrites the software image in flash memory with the downloaded image.</td>
</tr>
<tr>
<td></td>
<td>• The <strong>/reload</strong> option reloads the system after downloading the image unless the configuration has been changed and not been saved.</td>
</tr>
<tr>
<td></td>
<td>• For [username[:password]], specify the username and password; these must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File By Using FTP” section on page B-30.</td>
</tr>
<tr>
<td></td>
<td>• For @location, specify the IP address of the FTP server.</td>
</tr>
<tr>
<td></td>
<td>• For directory/image-name.tar, specify the directory (optional) and the image to download. Directory and image names are case sensitive.</td>
</tr>
</tbody>
</table>
Working with Software Images

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

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.

**Caution**
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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the FTP server is properly configured by referring to the “Preparing to Download or Upload a Configuration File By Using FTP” section on page B-13.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ip ftp username username</code> (Optional) Change the default remote username.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ip ftp password password</code> (Optional) Change the default password.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>end</code> Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td><code>archive upload-sw ftp://[[username]:password]@location[/directory]/image-name.tar</code> Upload the currently running switch image to the FTP server.</td>
</tr>
<tr>
<td></td>
<td>- For <code>[[username]:password]</code>, specify the username and password. These must be associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File By Using FTP” section on page B-30.</td>
</tr>
<tr>
<td></td>
<td>- For <code>@location</code>, specify the IP address of the FTP server.</td>
</tr>
<tr>
<td></td>
<td>- For <code>[/directory]/image-name.tar</code>, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The <code>image-name.tar</code> is the name of the software image to be stored on the server.</td>
</tr>
</tbody>
</table>

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.

⚠️ Caution

For the download and upload algorithms to operate properly, do not rename image names.
Copying Image Files By Using RCP

You can download a switch image from an RCP server or upload the image from the switch to an RCP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the same switch or another of the same type.

Note

Instead of using the copy privileged EXEC command or the archive tar privileged EXEC command, we recommend using the archive download-sw and archive upload-sw privileged EXEC commands to download and upload software image files.

These sections contain this configuration information:

- Preparing to Download or Upload an Image File By Using RCP, page B-34
- Downloading an Image File By Using RCP, page B-35
- Uploading an Image File By Using RCP, page B-37

Preparing to Download or Upload an Image File By 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 subnet network if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the `ping` command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the `show users` privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the `ip rcmd remote-username username` global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and there is no need to set the RCP username. Include the username in the `archive download-sw` or `archive upload-sw` privileged EXEC command if you want to specify a username only for that operation.
- When you upload an image to the RCP to the server, it must be properly configured to accept the RCP write request from the user on the switch. For UNIX systems, you must add an entry to the `.rhosts` file for the remote user on the RCP server.

For example, suppose the switch contains these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch IP address translates to `Switch1.company.com`, the `.rhosts` file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

## Downloading an Image File By 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload an Image File By Using RCP” section on page B-34.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Specify the remote username.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Appendix B  Working with the Cisco IOS File System, Configuration Files, and Software Images

Working with Software Images

Step 6

**Command**

```bash
archive download-sw /allow-feature-upgrade /overwrite /reload
rcp://[username@]location/directory/image-name.tar
```

**Purpose**

Download the image file from the RCP server to the switch, and overwrite the current image.

- The `/allow-feature-upgrade` option allows installation of an image with a different feature set.
- 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 more information, see the “Preparing to Download or Upload an Image File By Using RCP” section on page B-34.
- 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

**Command**

```bash
archive download-sw /leave-old-sw /reload
rcp://[username@]location/directory/image-name.tar
```

**Purpose**

Download the image file from the RCP 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 more information, see the “Preparing to Download or Upload an Image File By Using RCP” section on page B-34.
- 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 room 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 software 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.

⚠️ **Caution**

For the download and upload algorithms to operate properly, do not rename image names.

### Uploading an Image File By 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify that the RCP server is properly configured by referring to the “Preparing to Download or Upload an Image File By Using RCP” section on page B-34.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Log into the switch through the console port or a Telnet session.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).</td>
</tr>
<tr>
<td><code>ip rcmd remote-username</code></td>
<td>(Optional) Specify the remote username.</td>
</tr>
</tbody>
</table>
### Working with Software Images

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Upload the currently running switch image to the RCP server.</td>
</tr>
<tr>
<td>archive upload-sw rcp:</td>
<td></td>
</tr>
<tr>
<td>rcp://username@[location][directory]/image-name.tar]</td>
<td>For <strong>//username</strong>, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the “Preparing to Download or Upload an Image File By Using RCP” section on page B-34.</td>
</tr>
<tr>
<td></td>
<td>For <strong>@location</strong>, specify the IP address of the RCP server.</td>
</tr>
<tr>
<td></td>
<td>For <strong>/directory</strong>/image-name.tar, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive.</td>
</tr>
<tr>
<td></td>
<td>The <strong>image-name.tar</strong> is the name of software image to be stored on the server.</td>
</tr>
</tbody>
</table>

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.

⚠️ **Caution**

For the download and upload algorithms to operate properly, do not rename image names.
Unsupported Commands in Cisco IOS Release 12.2(55)SE

This appendix lists some of the command-line interface (CLI) commands that appear when you enter the question mark (?) at the Catalyst 3560 switch prompt but are not supported in this release, either because they are not tested or because of switch hardware limitations. This is not a complete list. These unsupported commands are listed by software feature and command mode:

- Access Control Lists, page C-2
- Archive Commands, page C-2
- Boot Loader Commands, page C-3
- Embedded Event Manager, page C-3
- Debug Commands, page C-4
- FallBack Bridging, page C-4
- High Availability, page C-6
- HSRP, page C-6
- IGMP Snooping Commands, page C-6
- Interface Commands, page C-7
- IP Multicast Routing, page C-7
- IP SLA, page C-8
- IP Unicast Routing, page C-9
- IPv6, page C-11
- Layer 3, page C-11
- MAC Address Commands, page C-13
- Miscellaneous, page C-14
- MSDP, page C-14
- Multicast, page C-15
- NetFlow Commands, page C-15
- Network Address Translation (NAT) Commands, page C-15
- QoS, page C-16
- RADIUS, page C-16
Access Control Lists

Unsupported Privileged EXEC Commands

- access-enable [host] [timeout minutes]
- access-template [access-list-number | name] [dynamic-name] [source] [destination] [timeout minutes]
- clear access-template [access-list-number | name] [dynamic-name] [source] [destination].
- show access-lists rate-limit [destination]
- show accounting
- show ip accounting [checkpoint] [output-packets | access violations]
- show ip cache [prefix-mask] [type number]

Unsupported Global Configuration Commands

- access-list rate-limit acl-index {precedence | mask prec-mask}
- access-list dynamic extended

Unsupported Route-Map Configuration Commands

- match ip address prefix-list prefix-list-name [prefix-list-name...]

Archive Commands

Unsupported Privileged EXEC Commands

- archive config
- logging persistent
- show archive config
- show archive log
ARP Commands

Unsupported Global Configuration Commands

arp ip-address hardware-address smds
arp ip-address hardware-address srp-a
arp ip-address hardware-address srp-b

Unsupported Interface Configuration Commands

arp probe
ip probe proxy

Boot Loader Commands

Unsupported Global Configuration Commands

boot buffersize

Embedded Event Manager

Unsupported Privileged EXEC Commands

event manager update user policy [policy-filename | group [group name expression]] | repository [url location]

Parameters are not supported for this command:
event manager run [policy name] [<paramater1>|...</paramater15]|

Unsupported Global Configuration Commands

no event manager directory user repository [url location]
event manager applet [applet-name] maxrun
Unsupported Commands in Applet Configuration Mode

**no event interface name** [interface-name] parameter [counter-name] entry-val [entry counter value] entry-op {gt|ge|eq|ne|lt|le} entry-type {increment | rate | value} [exit-val] exit-op {gt|ge|eq|ne|lt|le} exit-type {increment | rate | value} [average-factor <average-factor-value>]

**no trigger**

**tag**

### Debug Commands

#### Unsupported Privileged EXEC Commands

- `debug platform cli-redirection main`
- `debug platform configuration`

### FallBack Bridging

#### Unsupported Privileged EXEC Commands

- `clear bridge [bridge-group] multicast [router-ports | groups | counts] [group-address] [interface-unit] [counts]`
- `clear vlan statistics`
- `show bridge [bridge-group] circuit-group [circuit-group] [src-mac-address] [dst-mac-address]`
- `show bridge [bridge-group] multicast [router-ports | groups] [group-address]`
- `show bridge vlan`
- `show interfaces crb`
- `show interfaces [ethernet | fastethernet] [interface | slot/port] irb`
- `show subscriber-policy range`

### Unsupported Global Configuration Commands

- `bridge bridge-group acquire`
- `bridge bridge-group address mac-address [forward | discard] [interface-id]`
- `bridge bridge-group aging-time seconds`
- `bridge bridge-group bitswap_l3_addresses`
- `bridge bridge-group bridge ip`
- `bridge bridge-group circuit-group circuit-group pause milliseconds`
- `bridge bridge-group circuit-group circuit-group source-based`
bridge cmf
bridge crb
bridge bridge-group domain domain-name
bridge irb
bridge bridge-group mac-address-table limit number
bridge bridge-group multicast-source
bridge bridge-group protocol dec
bridge bridge-group route protocol
bridge bridge-group subscriber policy policy
subscriber-policy policy [no | default] packet [permit | deny]]

Unsupported Interface Configuration Commands

bridge-group bridge-group cbus-bridging
bridge-group bridge-group circuit-group circuit-number
bridge-group bridge-group input-address-list access-list-number
bridge-group bridge-group input-lat-service-deny group-list
bridge-group bridge-group input-lat-service-permit group-list
bridge-group bridge-group input-lsap-list access-list-number
bridge-group bridge-group input-pattern-list access-list-number
bridge-group bridge-group input-type-list access-list-number
bridge-group bridge-group lat-compression
bridge-group bridge-group output-address-list access-list-number
bridge-group bridge-group output-lat-service-deny group-list
bridge-group bridge-group output-lat-service-permit group-list
bridge-group bridge-group output-lsap-list access-list-number
bridge-group bridge-group output-pattern-list access-list-number
bridge-group bridge-group output-type-list access-list-number
bridge-group bridge-group sse
bridge-group bridge-group subscriber-loop-control
bridge-group bridge-group subscriber-trunk
bridge bridge-group lat-service-filtering
frame-relay map bridge dlei broadcast
interface bvi bridge-group
x25 map bridge x.121-address broadcast [options-keywords]
High Availability

Unsupported SSO-Aware HSRP Commands

All

HSRP

Unsupported Global Configuration Commands

interface Async
interface BVI
interface Dialer
interface Group-Async
interface Lex
interface Multilink
interface Virtual-Template
interface Virtual-Tokenring

Unsupported Interface Configuration Commands

mtu
standby mac-refresh seconds
standby use-bia

IGMP Snooping Commands

Unsupported Global Configuration Commands

ip igmp snooping tcn
Interface Commands

Unsupported Privileged EXEC Commands

show interfaces [interface-id | vlan vlan-id] [crb | fair-queue | irb | mac-accounting | precedence | irb | random-detect | rate-limit | shape]

Unsupported Global Configuration Commands

interface tunnel

Unsupported Interface Configuration Commands

transmit-interface type number

IP Multicast Routing

Unsupported Privileged EXEC Commands

clear ip rtp header-compression [type number]
The debug ip packet command displays packets received by the switch CPU. It does not display packets that are hardware-switched.
The debug ip mcache command affects packets received by the switch CPU. It does not display packets that are hardware-switched.
The debug ip mpacket [detail] [access-list-number [group-name-or-address] command affects only packets received by the switch CPU. Because most multicast packets are hardware-switched, use this command only when you know that the route will forward the packet to the CPU.
debug ip pim atm
show frame-relay ip rtp header-compression [interface type number]
The show ip mcache command displays entries in the cache for those packets that are sent to the switch CPU. Because most multicast packets are switched in hardware without CPU involvement, you can use this command, but multicast packet information is not displayed.
The show ip mpacket commands are supported but are only useful for packets received at the switch CPU. If the route is hardware-switched, the command has no effect because the CPU does not receive the packet and cannot display it.
show ip pim vc [group-address | name] [type number]
show ip rtp header-compression [type number] [detail]
Unsupported Global Configuration Commands

ip pim accept-rp {address | auto-rp} [group-access-list-number]

ip pim message-interval seconds

Unsupported Interface Configuration Commands

frame-relay ip rtp header-compression {active | passive}
frame-relay map ip ip-address dlei [broadcast] compress
frame-relay map ip ip-address dlei rtp header-compression {active | passive}

ip igmp helper-address ip-address

ip multicast helper-map {group-address | broadcast} {broadcast-address | multicast-address}

ip multicast map ip ip-address dlei [broadcast] [compress]

ip multicast map ip ip-address dlei rtp header-compression {active | passive}

ip igmp helper-address ip-address

ip multicast helper-map {group-address | broadcast} {broadcast-address | multicast-address}

ip multicast rate-limit {in | out} [video | whiteboard] [group-list access-list] [source-list access-list]

ip multicast rate-limit {in | out} [video | whiteboard] [group-list access-list] [source-list access-list]

ip multicast ttl-threshold ttl-value (instead, use the ip multicast boundary access-list-number interface configuration command)

ip multicast use-functional

ip pim minimum-vc-rate pps

ip pim multipoint-signalling

ip pim nbma-mode

ip pim vc-count number

ip rtp compression-connections number

ip rtp header-compression [passive]

IP SLA

Unsupported MPLS Health Monitor Commands

All

Unsupported Ethernet Gatekeeper Registration Commands

All

Unsupported VoIP Call Setup Probe Commands

All
IP Unicast Routing

Unsupported Privileged EXEC or User EXEC Commands

- clear ip accounting [checkpoint]
- clear ip bgp address flap-statistics
- clear ip bgp prefix-list
- debug ip cef stats
- show cef [drop | not-cef-switched]
- show ip accounting [checkpoint] [output-packets | access-violations]
- show ip bgp dampened-paths
- show ip bgp inconsistent-as
- show ip bgp regexp regular expression
- show ip prefix-list regular expression

Unsupported Global Configuration Commands

- ip accounting precedence {input | output}
- ip accounting-list ip-address wildcard
- ip as-path access-list
- ip accounting-transits count
- ip cef traffic-statistics [load-interval seconds] [update-rate seconds]
- ip flow-aggregation
- ip flow-cache
- ip flow-export
- ip gratuitous-arps
- ip local
- ip prefix-list
- ip reflexive-list
- router egp
- router-isis
- router iso-igrp
- router mobile
- router odr
- router static
Unsupported Interface Configuration Commands

ip accounting
ip load-sharing [per-packet]
ip mtu bytes
ip ospf dead-interval minimal hello-multiplier multiplier
ip verify
ip unnumbered type number
All ip security commands

Unsupported BGP Router Configuration Commands

address-family vpnv4
default-information originate
neighbor advertise-map
neighbor allowas-in
neighbor default-originate
neighbor description
network backdoor
table-map

Unsupported VPN Configuration Commands

All

Unsupported Route Map Commands

match route-type for policy-based routing (PBR)
set as-path {tag | prepend as-path-string}
set automatic-tag
set dampening half-life reuse suppress max-suppress-time
set default interface interface-id [interface-id.....]
set interface interface-id [interface-id.....]
set ip default next-hop ip-address [ip-address.....]
set ip destination ip-address mask
set ip next-hop verify-availability
set ip precedence value
set ip qos-group
set metric-type internal
set origin
set metric-type internal
set tag tag-value

IPv6

IPv4-v6 Tunneling Commands

All

Layer 3

BGP

All commands for these features:
- BGP Support for Dual AS Configuration for Network AS Migrations
- BGP Support for IP Prefix Import from Global Table into a VRF Table
- BGP Support for Named Extended Community Lists
- BGP Support for Sequenced Entries in Extended Community Lists
- BGP Support for TTL Security Check
- BGP Route-Map Policy List Support
- BGP Next Hop Propagation
- BGP Policy Accounting
- BGP Policy Accounting output interface accounting
- BGP Link Bandwidth
- BGP Hybrid CLI Support
- BGP Cost Community
- BGP Dynamic Update Peer-Groups
- BGP Conditional Route Injection
- BGP Configuration Using Peer Templates
- BGP Increased Support of Numbered as-path Access Lists to 500

Other Unsupported BGP Commands

address-family l2vpn
address-family vpnv4
bgp-policyclear bgp nsapaddress-family nsap
clear bgp nsap dampening
clear bgp nsap external
clear bgp nsap flap-statistics
clear bgp nsap peer-group
clear ip bgp ipv6
clear ip bgp l2vpn
clear ip bgp vpnv4
clear ip bgp vpnv6
ha-mode graceful-restart
ip extcommunity-list redistribute (BGP to ISO IS-IS)
ip policy-list redistribute (ISO IS-IS to BGP)
match extcommunity
neighbor ha-mode graceful-restart
neighbor soo redistribute dvmrp
neighbor ttl-securityset extcommunity
set extcommunity cost
show bgp nsap
show bgp nsap community
show bgp nsap community-list
show bgp nsap dampening
show bgp nsap dampened-paths
show bgp nsap filter-list
show bgp nsap flap-statistics
show bgp nsap inconsistent-as
show bgp nsap neighbors
show bgp nsap paths
show bgp nsap quote-regexp
show bgp nsap regexp
show bgp nsap summary
show ip bgp ipv4 multicast
show ip bgp ipv4 multicast summary
show ip bgp l2vpn
show ip bgp vpnv4
show ip extcommunity-list
show ip policy-list
OSPF

area sham-link
ignore lsa mospf
nsf ietf
nsf ietf helper disable
nsf ietf helper strict-lsa-checking
show ip ospf sham-links

VRF aware AAA

All

MAC Address Commands

Unsupported Privileged EXEC Commands

show mac-address-table
show mac-address-table address
show mac-address-table aging-time
show mac-address-table count
show mac-address-table dynamic
show mac-address-table interface
show mac-address-table multicast
show mac-address-table notification
show mac-address-table static
show mac-address-table vlan
show mac address-table multicast

Note Use the show ip igmp snooping groups privileged EXEC command to display Layer 2 multicast address-table entries for a VLAN.

Unsupported Global Configuration Commands

mac-address-table aging-time
mac-address-table notification
mac-address-table static
Miscellaneous

Unsupported User EXEC Commands

verify

Unsupported Privileged EXEC Commands

file verify auto
remote command
show cable-diagnostics prbs
test cable-diagnostics prbs

Unsupported Global Configuration Commands

ero disable recovery cause unicast flood
l2protocol-tunnel global drop-threshold
memory reserve critical
service compress-config
track object-number rtr
stack-mac persistent timer

MSDP

Unsupported Privileged EXEC Commands

show access-expression
show exception
show location
show pm LINE
show smf [interface-id]
show subscriber-policy [policy-number]
show template [template-name]

Unsupported Global Configuration Commands

ip msdp default-peer ip-address | name [prefix-list list] (Because BGP/MBGP is not supported, use the ip msdp peer command instead of this command.)
Multicast

Unsupported BiDirectional PIM Commands
All

Unsupported Multicast Routing Manager Commands
All

Unsupported IP Multicast Rate Limiting Commands
All

Unsupported UDLR Commands
All

Unsupported Multicast Over GRE Commands
All

NetFlow Commands

Unsupported Global Configuration Commands
  ip flow-aggregation cache
  ip flow-cache entries
  ip flow-export

Network Address Translation (NAT) Commands

Unsupported Privileged EXEC Commands
  show ip nat statistics
  show ip nat translations
QoS

Unsupported Global Configuration Command

priority-list

Unsupported Interface Configuration Commands

priority-group
rate-limit

Unsupported Policy-Map Configuration Command

class class-default where class-default is the class-map-name.

RADIUS

Unsupported Global Configuration Commands

aaa nas port extended
aaa authentication feature default enable
aaa authentication feature default line
aaa nas port extended
radius-server attribute nas-port
radius-server configure
radius-server extended-portnames

SNMP

Unsupported Global Configuration Commands

snmp-server enable informs
snmp-server ifindex persist
SNMPv3

Unsupported 3DES Encryption Commands

All

Spanning Tree

Unsupported Global Configuration Command

spanning-tree pathcost method {long | short}

Unsupported Interface Configuration Command

spanning-tree stack-port

VLAN

Unsupported Global Configuration Command

vlan internal allocation policy {ascending | descending}

Unsupported User EXEC Commands

show running-config vlan
show vlan ifindex
vlan database

Unsupported VLAN Database Commands

vtp
vlan
VTP

Unsupported Privileged EXEC Commands

```
vtp {password password | pruning | version number}
```

**Note**
This command has been replaced by the `vtp` global configuration command.