INDEX

Numerics

802.1AE Tagging 7-2

A

abbreviating commands 2-3
AC (command switch) 8-9
access-class command 33-17
access control entries
  See ACEs
access control entry (ACE) 38-3
access-denied response, VMPS 14-24
accessing
  clusters, switch 8-12
  command switches 8-10
  member switches 8-12
  switch clusters 8-12
accessing stack members 9-21
access lists
  See ACLs
access ports
  in switch clusters 8-8
accounting
  with 802.1x 12-52
  with IEEE 802.1x 12-16
  with RADIUS 11-35
  with TACACS+ 11-12, 11-17
ACEs
  and QoS 34-7
  defined 33-1
  Ethernet 33-2
  IP 33-2
ACLs
  ACEs 33-1
  any keyword 33-9
  applying
    time ranges to 33-14
    to an interface 33-17, 38-7
    to IPv6 interfaces 38-7
    to QoS 34-7
  classifying traffic for QoS 34-43
  comments in 33-16
  compiling 33-20
  defined 33-1, 33-5
  examples of 33-20, 34-43
  extended IP, configuring for QoS classification 34-45
  extended IPv4
    creating 33-8
    matching criteria 33-6
  hardware and software handling 33-18
  host keyword 33-10
  IP
    creating 33-5
    fragments and QoS guidelines 34-34
    implicit deny 33-7, 33-12, 33-13
    implicit masks 33-7
    matching criteria 33-6
    undefined 33-18
  IPv4
    applying to interfaces 33-17
    creating 33-5
    matching criteria 33-6
    named 33-12
    numbers 33-6
    terminal lines, setting on 33-17

unsupported features 33-5
IPv6
applying to interfaces 38-7
configuring 38-3, 38-4
displaying 38-8
interactions with other features 38-4
limitations 38-2, 38-3
matching criteria 38-3
named 38-2
precedence of 38-2
supported 38-2
unsupported features 38-3
MAC extended 33-21, 34-46
matching 33-5, 33-18, 38-3
monitoring 33-24, 38-8
named, IPv4 33-12
named, IPv6 38-2
names 38-4
number per QoS class map 34-35
port 33-2, 38-1
QoS 34-7, 34-43
resequencing entries 33-12
router 33-2, 38-1
standard IP, configuring for QoS classification 34-44
standard IPv4
creating 33-7
matching criteria 33-6
support in hardware 33-18
time ranges 33-14
types supported 33-2
unsupported features, IPv4 33-5
unsupported features, IPv6 38-3
active link 20-4, 20-5
active links 20-1
active traffic monitoring, IP SLAs 32-1
address aliasing 23-2
addresses
displaying the MAC address table 5-23
dynamic
accelerated aging 17-8
changing the aging time 5-15
default aging 17-8
defined 5-13
learning 5-14
removing 5-16
IPv6 36-2
MAC, discovering 5-24
static
adding and removing 5-20
defined 5-13
address resolution 5-24
Address Resolution Protocol
See ARP
advertisements
CDP 26-1
LLDP 27-1, 27-2
VTP 14-15, 15-3
aggregatable global unicast addresses 36-3
aggregated ports
See EtherChannel
aggregate policers 34-54
aggregate policing 1-10
aging, accelerating 17-8
aging time
accelerated
for MSTP 18-23
for STP 17-8, 17-21
MAC address table 5-15
maximum
for MSTP 18-24
for STP 17-21, 17-22
alarms, RMON 29-4
allowed-VLAN list 14-17
ARP
defined 1-5, 5-24
table
address resolution 5-24
managing 5-24

attributes, RADIUS
vendor-proprietary 11-38
vendor-specific 11-36
attribute-value pairs 12-13, 12-16, 12-21, 12-22
authentication
local mode with AAA 11-40
open1x 12-30
RADIUS
key 11-28
login 11-30
TACACS+
defined 11-11
key 11-13
login 11-14
See also port-based authentication
authentication compatibility with Catalyst 6000 switches 12-8
authentication failed VLAN
See restricted VLAN
authentication manager
CLI commands 12-9
compatibility with older 802.1x CLI commands 12-9 to ??
overview 12-7
authoritative time source, described 5-2
authorization
with RADIUS 11-34
with TACACS+ 11-12, 11-16
authorized ports with IEEE 802.1x 12-10
autoconfiguration 3-3
auto enablement 12-32
automatic advise (auto-advise) in switch stacks 9-10
automatic copy (auto-copy) in switch stacks 9-10
automatic discovery
considerations
beyond a noncandidate device 8-7
brand new switches 8-8
connectivity 8-4
different VLANs 8-6
management VLANs 8-7
non-CDP-capable devices 8-5
noncluster-capable devices 8-5
in switch clusters 8-4
See also CDP
automatic extraction (auto-extract) in switch stacks 9-10
automatic QoS
See QoS
automatic recovery, clusters 8-9
See also HSRP
automatic upgrades (auto-upgrade) in switch stacks 9-10
auto-MDIX
configuring 13-15
described 13-15
autonegotiation
duplex mode 1-3
interface configuration guidelines 13-12
mismatches 40-11
Auto-QoS video devices 1-11
autosensing, port speed 1-3
auxiliary VLAN
See voice VLAN
availability, features 1-6

B

BackboneFast
described 19-5
disabling 19-14
enabling 19-13
backup interfaces
See Flex Links
backup links 20-1
banners
configuring
login 5-13
message-of-the-day login 5-11
default configuration 5-11
when displayed 5-11

Berkeley r-tools replacement 11-52
binding database
DHCP snooping
See DHCP snooping binding database
bindings
DHCP snooping database 21-6
IP source guard 21-12
binding table, DHCP snooping
See DHCP snooping binding database
blocking packets 24-7
booting
boot loader, function of 3-1
boot process 3-1
manually 3-19
specific image 3-20
boot loader
accessing 3-21
described 3-1
environment variables 3-21
prompt 3-21
trap-door mechanism 3-2
Boot Loader Upgrade and Image Verification for the FIPS Mode of Operation 3-24
BPDU
error-disabled state 19-2
filtering 19-3
RSTP format 18-12
BPDU filtering
described 19-3
disabling 19-12
enabling 19-12
support for 1-7
BPDU guard
described 19-2
disabling 19-12
enabling 19-11
support for 1-7
bridge protocol data unit
See BPDU
broadcast storm-control command 24-4
broadcast storms 24-1

C

cables, monitoring for unidirectional links 25-1
candidate switch
automatic discovery 8-4
defined 8-3
requirements 8-3
See also command switch, cluster standby group, and member switch
Catalyst 6000 switches
authentication compatibility 12-8
CA trustpoint
configuring 11-49
defined 11-47
CDP
and trusted boundary 34-39
automatic discovery in switch clusters 8-4
configuring 26-2
default configuration 26-2
defined with LLDP 27-1
described 26-1
disabling for routing device 26-4
enabling and disabling
on an interface 26-4
on a switch 26-4
monitoring 26-5
overview 26-1
power negotiation extensions 13-4
support for 1-5
transmission timer and holdtime, setting 26-3
updates 26-3
CGMP
as IGMP snooping learning method 23-8
joining multicast group 23-3
CipherSuites 11-48
Cisco 7960 IP Phone 16-1

Cisco Discovery Protocol
See CDP
Cisco intelligent power management 13-4
Cisco IOS File System
See IFS
Cisco IOS IP SLAs 32-1
Cisco Secure ACS
attribute-value pairs for downloadable ACLs 12-22
attribute-value pairs for redirect URL 12-21
Cisco Secure ACS configuration guide 12-63
CiscoWorks 2000 1-4, 31-4
CISP 12-32
CIST regional root
See MSTP
CIST root
See MSTP
civic location 27-3
class maps for QoS
configuring 34-47
described 34-7
displaying 34-74
class of service
See CoS
clearing interfaces 13-21
CLI
abbreviating commands 2-3
command modes 2-1
configuration logging 2-5
described 1-4
editing features
enabling and disabling 2-6
keystroke editing 2-7
wrapped lines 2-8
error messages 2-4
filtering command output 2-9
getting help 2-3
history
changing the buffer size 2-5
described 2-5
disabling 2-6
recalling commands 2-6
managing clusters 8-13
no and default forms of commands 2-4
Client Information Signalling Protocol
See CISP
client mode, VTP 15-3
clock
See system clock
clusters, switch
accessing 8-12
automatic discovery 8-4
automatic recovery 8-9
benefits 1-1
compatibility 8-4
described 8-1
LRE profile considerations 8-13
managing
through CLI 8-13
through SNMP 8-14
planning 8-4
planning considerations
automatic discovery 8-4
automatic recovery 8-9
CLI 8-13
host names 8-12
IP addresses 8-12
LRE profiles 8-13
passwords 8-12
RADIUS 8-13
SNMP 8-13, 8-14
TACACS+ 8-13
See also candidate switch, command switch, cluster standby group, member switch, and standby command switch
cluster standby group
automatic recovery 8-11
considerations 8-10
defined 8-2

requirements 8-3
virtual IP address 8-10
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 4-8
management functions 1-4
CoA Request Commands 11-23
Coarse Wave Division Multiplexer
See CWDM SFPs
command-line interface
See CLI
command modes 2-1
commands
abbreviating 2-3
no and default 2-4
commands, setting privilege levels 11-8
command switch
accessing 8-10
active (AC) 8-9
configuration conflicts 40-11
defined 8-2
passive (PC) 8-9
password privilege levels 8-14
priority 8-9
recovery
from command-switch failure 8-9, 40-8
from lost member connectivity 40-11
redundant 8-9
replacing
with another switch 40-10
with cluster member 40-8
requirements 8-3
standby (SC) 8-9
See also candidate switch, cluster standby group, member switch, and standby command switch
community strings
configuring 8-13, 31-9
for cluster switches 31-4
in clusters 8-13
overview 31-4
SNMP 8-13
compatibility, feature 24-12
compatibility, software
See stacks, switch
config.text 3-18
configurable leave timer, IGMP 23-5
configuration, initial
defaults 1-12
Express Setup 1-1
configuration changes, logging 30-10
configuration conflicts, recovering from lost member connectivity 40-11
configuration examples, network 1-14
configuration files
archiving 42-20
clearing the startup configuration 42-19
creating using a text editor 42-9
default name 3-18
deleting a stored configuration 42-19
described 42-8
downloading
automatically 3-18
preparing 42-10, 42-13, 42-16
reasons for 42-8
using FTP 42-13
using RCP 42-17
using TFTP 42-11
guidelines for creating and using 42-8
guidelines for replacing and rolling back 42-21

invalid combinations when copying 42-5
limiting TFTP server access 31-18
obtaining with DHCP 3-8
password recovery disable considerations 11-5
replacing a running configuration 42-19, 42-20
rolling back a running configuration 42-19, 42-21
specifying the filename 3-18
system contact and location information 31-18
types and location 42-9
uploading
preparing 42-10, 42-13, 42-16
reasons for 42-8
using FTP 42-15
using RCP 42-18
using TFTP 42-12
configuration logger 30-10
configuration logging 2-5
configuration replacement 42-19
configuration rollback 42-19, 42-20
configuration settings, saving 3-15
configure terminal command 13-7
configuring 802.1x user distribution 12-58
configuring port-based authentication violation modes 12-41
configuring small-frame arrival rate 24-5
conflicts, configuration 40-11
connections, secure remote 11-42
connectivity problems 40-13, 40-14, 40-16
consistency checks in VTP Version 2 15-4
console port, connecting to 2-9
control protocol, IP SLAs 32-3
corrupted software, recovery steps with Xmodem 40-2
CoS
in Layer 2 frames 34-2
override priority 16-6
trust priority 16-6
CoS input queue threshold map for QoS 34-13
CoS output queue threshold map for QoS 34-15
CoS-to-DSCP map for QoS 34-56
counters, clearing interface 13-21
CPU utilization, troubleshooting 40-24
crashinfo file 40-22
critical authentication, IEEE 802.1x 12-55
critical VLAN 12-24
critical voice VLAN
configuring 12-55
cryptographic software image
SSH 11-41
SSL 11-46
switch stack considerations 9-14
customjzeable web pages, web-based authentication 6-6
CWDM SFPs 1-16

D

DACL
See downloadable ACL
daylight saving time 5-7
debugging
enabling all system diagnostics 40-20
enabling for a specific feature 40-19
redirecting error message output 40-20
using commands 40-18
default commands 2-4
default configuration
802.1x 12-35
auto-QoS 34-17
banners 5-11
CDP 26-2
DHCP 21-7
DHCP option 82 21-8
DHCP snooping 21-8
DHCP snooping binding database 21-8
DNS 5-10
dynamic ARP inspection 22-5
EtherChannel 39-9
Ethernet interfaces 13-11
Flex Links 20-8

IGMP filtering 23-24
IGMP snooping 23-6, 37-6
IGMP throttling 23-24
initial switch information 3-3
IP SLAs 32-5
IP source guard 21-14
IPv6 36-7
Layer 2 interfaces 13-11
LLDP 27-4
MAC address table 5-15
MAC address-table move update 20-8
MSTP 18-14
MVR 23-19
optional spanning-tree configuration 19-9
password and privilege level 11-2
RADIUS 11-27
RMON 29-3
RSPAN 28-9
SNMP 31-8
SPAN 28-9
SSL 11-48
standard QoS 34-32
STP 17-11
switch stacks 9-16
system message logging 30-3
system name and prompt 5-9
TACACS+ 11-13
UDLD 25-4
VLAN, Layer 2 Ethernet interfaces 14-15
VLANs 14-8
VMPS 14-25
voice VLAN 16-3
VTP 15-7
default gateway 3-14
default web-based authentication configuration
802.1X 6-9
deleting VLANs 14-9
denial-of-service attack 24-1
description command 13-18
designing your network, examples 1-14
destination addresses
in IPv4 ACLs 33-9
in IPv6 ACLs 38-5
destination-IP address-based forwarding, EtherChannel 39-7
destination-MAC address forwarding, EtherChannel 39-7
detecting indirect link failures, STP 19-5
device 42-24
device discovery protocol 26-1, 27-1
device manager
benefits 1-1
described 1-2, 1-4
in-band management 1-5
upgrading a switch 42-24
DHCP
enabling
relay agent 21-9
DHCP-based autoconfiguration
client request message exchange 3-4
configuring
client side 3-3
DNS 3-7
relay device 3-7
server side 3-6
TFTP server 3-7
example 3-9
lease options
for IP address information 3-6
for receiving the configuration file 3-6
overview 3-3
relationship to BOOTP 3-3
relay support 1-5
support for 1-5
DHCP-based autoconfiguration and image update
configuring 3-11 to 3-14
understanding 3-5
DHCP binding database
See DHCP snooping binding database

DHCP binding table
See DHCP snooping binding database
DHCP option 82
circuit ID suboption 21-5
configuration guidelines 21-8
default configuration 21-7
displaying 21-12
overview 21-3
packet format, suboption
circuit ID 21-5
remote ID 21-5
remote ID suboption 21-5
DHCP server port-based address allocation
configuration guidelines 21-21
default configuration 21-21
described 21-21
displaying 21-24
enabling 21-21
reserved addresses 21-22
DHCP server port-based address assignment
support for 1-5
DHCP snooping
accepting untrusted packets form edge switch 21-3, 21-10
binding database
See DHCP snooping binding database
configuration guidelines 21-8
default configuration 21-7
displaying binding tables 21-12
message exchange process 21-4
option 82 data insertion 21-3
trusted interface 21-2
untrusted interface 21-2
untrusted messages 21-2
DHCP snooping binding database
adding bindings 21-11
binding file
format 21-6
location 21-6
bindings 21-6
clearing agent statistics 21-12
configuration guidelines 21-8
configuring 21-11
default configuration 21-7, 21-8
deleting
binding file 21-12
bindings 21-12
database agent 21-12
described 21-6
displaying 21-12
enabling 21-11
entry 21-6
renewing database 21-12
resetting
delay value 21-12
timeout value 21-12
DHCP snooping binding table
See DHCP snooping binding database
Differentiated Services architecture, QoS 34-1
Differentiated Services Code Point 34-2
directed unicast requests 1-5
directories
changing 42-3
creating and removing 42-4
displaying the working 42-3
discovery, clusters
See automatic discovery
DNS
and DHCP-based autoconfiguration 3-7
default configuration 5-10
displaying the configuration 5-11
in IPv6 36-3
overview 5-9
setting up 5-10
support for 1-5
domain names
DNS 5-9
VTP 15-8

Domain Name System
See DNS
downloadable ACL 12-20, 12-22, 12-63
downloading
configuration files
preparing 42-10, 42-13, 42-16
reasons for 42-8
using FTP 42-13
using RCP 42-17
using TFTP 42-11
image files
deleting old image 42-28
preparing 42-26, 42-29, 42-33
reasons for 42-24
using CMS 1-2
using FTP 42-30
using HTTP 1-2, 42-24
using RCP 42-34
using TFTP 42-26
using the device manager or Network Assistant 42-24
DSCP 1-10, 34-2
DSCP input queue threshold map for QoS 34-13
DSCP output queue threshold map for QoS 34-15
DSCP-to-CoS map for QoS 34-59
DSCP-to-DSCP-mutation map for QoS 34-60
DSCP transparency 34-40
DTP 1-7, 14-14
dual-action detection 39-4
dual IPv4 and IPv6 templates 36-6
dual protocol stacks
IPv4 and IPv6 36-6
SDM templates supporting 36-6
dynamic access ports
characteristics 14-4
configuring 14-26
defined 13-2
dynamic addresses
See addresses
dynamic ARP inspection
ARP cache poisoning 22-1
ARP requests, described 22-1
ARP spoofing attack 22-1
clearing
log buffer 22-16
statistics 22-16
configuration guidelines 22-5
configuring
ACLs for non-DHCP environments 22-9
in DHCP environments 22-6
log buffer 22-13
rate limit for incoming ARP packets 22-4, 22-11
default configuration 22-5
denial-of-service attacks, preventing 22-11
described 22-1
DHCP snooping binding database 22-2
displaying
ARP ACLs 22-16
configuration and operating state 22-16
log buffer 22-16
statistics 22-16
trust state and rate limit 22-16
error-disabled state for exceeding rate limit 22-4
function of 22-2
interface trust states 22-3
log buffer
clearing 22-16
configuring 22-13
displaying 22-16
logging of dropped packets, described 22-4
man-in-the middle attack, described 22-2
network security issues and interface trust states 22-3
priority of ARP ACLs and DHCP snooping entries 22-4
rate limiting of ARP packets
configuring 22-11
described 22-4
error-disabled state 22-4

statistics
clearing 22-16
displaying 22-16
validation checks, performing 22-13
dynamic auto trunking mode 14-14
dynamic desirable trunking mode 14-14
Dynamic Host Configuration Protocol
See DHCP-based autoconfiguration
dynamic port VLAN membership
described 14-24
reconfirming 14-27
troubleshooting 14-29
types of connections 14-26
Dynamic Trunking Protocol
See DTP

E

EAC 7-2
editing features
enabling and disabling 2-6
keystrokes used 2-7
wrapped lines 2-8
elections
See stack master
ELIN location 27-3
enable password 11-3
enable secret password 11-3
encryption, CipherSuite 11-48
encryption for passwords 11-3
Endpoint Admission Control (EAC) 7-2
environment variables, function of 3-22
error-disabled state, BPDU 19-2
error messages during command entry 2-4
EtherChannel
automatic creation of 39-3, 39-5
channel groups
numbering of 39-3
configuration guidelines 39-9
default configuration 39-9
described 39-2
displaying status 39-17
forwarding methods 39-6, 39-12
IEEE 802.3ad, described 39-5
interaction
with STP 39-9
with VLANs 39-10
LACP
described 39-5
displaying status 39-17
hot-standby ports 39-14
interaction with other features 39-6
modes 39-5
port priority 39-15
system priority 39-15
load balancing 39-6, 39-12
PAgP
aggregate-port learners 39-13
compatibility with Catalyst 1900 39-13
described 39-3
displaying status 39-17
interaction with other features 39-5
interaction with virtual switches 39-4
learn method and priority configuration 39-13
modes 39-4
support for 1-3
with dual-action detection 39-4
port-channel interfaces
described 39-3
numbering of 39-3
port groups 13-3
support for 1-3
EtherChannel guard
described 19-7
disabling 19-14
enabling 19-14
Ethernet VLANs
adding 14-8

defaults and ranges 14-8
modifying 14-8
EUI 36-3
events, RMON 29-4
examples
network configuration 1-14
expedite queue for QoS 34-73
Express Setup 1-1
See also getting started guide
extended crashinfo file 40-22
extended-range VLANs
configuration guidelines 14-11
configuring 14-11
creating 14-12
defined 14-1
extended system ID
MSTP 18-17
STP 17-4, 17-14
extended universal identifier
See EUI
Extensible Authentication Protocol over LAN 12-1

F

fa0 interface 1-5
Fast Convergence 20-3
features, incompatible 24-12
fiber-optic, detecting unidirectional links 25-1
files
basic crashinfo
description 40-22
location 40-22
copying 42-4
crashinfo, description 40-22
deleting 42-5
displaying the contents of 42-7
extended crashinfo
description 40-23
location 40-23
tar
creating 42-6
displaying the contents of 42-6
extracting 42-7
image file format 42-25
file system
displaying available file systems 42-2
displaying file information 42-3
local file system names 42-1
network file system names 42-4
setting the default 42-3
filtering
IPv6 traffic 38-3, 38-7
non-IP traffic 33-21
show and more command output 2-9
filtering show and more command output 2-9
filters, IP
See ACLs, IP
flash device, number of 42-1
flexible authentication ordering
configuring 12-65
overview 12-30
Flex Link Multicast Fast Convergence 20-3
Flex Links
configuration guidelines 20-8
configuring 20-9
configuring preferred VLAN 20-11
configuring VLAN load balancing 20-10
default configuration 20-8
description 20-1
link load balancing 20-2
monitoring 20-14
VLANs 20-2
flooded traffic, blocking 24-8
flow-based packet classification 1-10
flowcharts
QoS classification 34-6
QoS egress queueing and scheduling 34-14
QoS ingress queueing and scheduling 34-12

QoS policing and marking 34-10
flowcontrol
configuring 13-14
described 13-14
forward-delay time
MSTP 18-23
STP 17-21
FTP
configuration files
downloading 42-13
overview 42-12
preparing the server 42-13
uploading 42-15
image files
deleting old image 42-32
downloading 42-30
preparing the server 42-29
uploading 42-32

G

general query 20-5
Generating IGMP Reports 20-3
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 23-12
guest VLAN and 802.1x 12-22
guide mode 1-2
GUIs
See device manager and Network Assistant

H

hello time
MSTP 18-23
STP 17-20
help, for the command line 2-3
HFTM space 40-23
history
changing the buffer size 2-5
described 2-5
disabling 2-6
recalling commands 2-6
history table, level and number of syslog messages 30-9
host names, in clusters 8-12
hosts, limit on dynamic ports 14-29
HP OpenView 1-4
HQATM space 40-23
HSRP
automatic cluster recovery 8-11
cluster standby group considerations 8-10
See also clusters, cluster standby group, and standby command switch
HTTP over SSL
see HTTPS
HTTPS 11-46
configuring 11-50
self-signed certificate 11-47
HTTP secure server 11-46
Hulc Forwarding TCAM Manager
See HFTM space
Hulc QoS/ACL TCAM Manager
See HQATM space

I

ICMP
IPv6 36-3
time-exceeded messages 40-16
traceroute and 40-16
unreachable messages and IPv6 38-4
ICMP ping
executing 40-13
overview 40-13

ICMPv6 36-3
IDS appliances
and ingress RSPAN 28-19
and ingress SPAN 28-12
IEEE 802.1D
See STP
IEEE 802.1p 16-1
IEEE 802.1Q
configuration limitations 14-15
native VLAN for untagged traffic 14-19
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 13-14
ifIndex values, SNMP 31-5
IFS 1-5
IGMP
configurable leave timer
described 23-5
enabling 23-10
flooded multicast traffic
controlling the length of time 23-11
disabling on an interface 23-12
global leave 23-12
query solicitation 23-12
recovering from flood mode 23-12
joining multicast group 23-3
join messages 23-3
leave processing, enabling 23-10, 37-9
leaving multicast group 23-5
queries 23-4
report suppression
described 23-6
disabling 23-15, 37-11
supported versions 23-2
IGMP filtering
configuring 23-24
default configuration 23-24
described 23-23
monitoring 23-28
support for 1-4
IGMP groups
configuring filtering 23-27
setting the maximum number 23-26
IGMP Immediate Leave
configuration guidelines 23-10
described 23-5
enabling 23-10
IGMP profile
applying 23-25
configuration mode 23-24
configuring 23-25
IGMP snooping
and address aliasing 23-2
configuring 23-6
default configuration 23-6, 37-6
definition 23-1
enabling and disabling 23-7, 37-7
global configuration 23-7
Immediate Leave 23-5
method 23-8
monitoring 23-16, 37-12
querier
configuration guidelines 23-13
configuring 23-13
supported versions 23-2
VLAN configuration 23-7
IGMP throttling
configuring 23-27
default configuration 23-24
described 23-24

displaying action 23-28
Immediate Leave, IGMP 23-5
enabling 37-9
inaccessible authentication bypass 12-24
support for multiauth ports 12-25
initial configuration
defaults 1-12
Express Setup 1-1
interface
range macros 13-9
interface command ?? to 13-7
interface configuration mode 2-2
interfaces
auto-MDIX, configuring 13-15
configuration guidelines
duplex and speed 13-12
configuring
procedure 13-7
counters, clearing 13-21
default configuration 13-11
described 13-18
descriptive name, adding 13-18
displaying information about 13-21
flow control 13-14
management 1-4
monitoring 13-20
naming 13-18
physical, identifying 13-7
range of 13-8
restarting 13-22
shutting down 13-22
speed and duplex, configuring 13-13
status 13-20
supported 13-7
types of 13-1
interfaces range macro command 13-9
interface types 13-7
Internet Protocol version 6
See IPv6
inter-VLAN routing 35-1
Intrusion Detection System
See IDS appliances
inventory management TLV 27-3, 27-7
IP ACLs
for QoS classification 34-7
implicit deny 33-7, 33-12
implicit masks 33-7
named 33-12
undefined 33-18
IP addresses
128-bit 36-2
candidate or member 8-3, 8-12
classes of 35-4
cluster access 8-2
command switch 8-3, 8-10, 8-12
discovering 5-24
for IP routing 35-4
IPv6 36-2
redundant clusters 8-10
standby command switch 8-10, 8-12
See also IP information
ip igmp profile command 23-24
IP information
assigned
manually 3-14
through DHCP-based autoconfiguration 3-3
default configuration 3-3
IP phones
and QoS 16-1
automatic classification and queueing 34-17
configuring 16-4
ensuring port security with QoS 34-39
trusted boundary for QoS 34-39
IP Port Security for Static Hosts
on a Layer 2 access port 21-16
IP precedence 34-2
IP-precedence-to-DSCP map for QoS 34-57
IP routing

disabling 35-4
enabling 35-4
IP Service Level Agreements
See IP SLAs
IP service levels, analyzing 32-1
IP SLAs
benefits 32-2
configuration guidelines 32-5
Control Protocol 32-3
default configuration 32-5
definition 32-1
measuring network performance 32-2
monitoring 32-6
operation 32-2
responder
described 32-3
enabling 32-5
response time 32-4
SNMP support 32-2
supported metrics 32-1
IP source guard
and 802.1x 21-15
and DHCP snooping 21-12
and port security 21-15
and private VLANs 21-15
and routed ports 21-15
and TCAM entries 21-15
and trunk interfaces 21-15
and VRF 21-15
binding configuration
automatic 21-12
manual 21-12
binding table 21-12
configuration guidelines 21-15
default configuration 21-14
described 21-12
disabling 21-16
displaying
active IP or MAC bindings 21-20
bindings 21-20
configuration 21-20
enabling 21-15, 21-16
filtering
source IP address 21-13
source IP and MAC address 21-13
source IP address filtering 21-13
source IP and MAC address filtering 21-13
static bindings
adding 21-15, 21-16
deleting 21-16
static hosts 21-16
IP traceroute
executing 40-17
overview 40-16
IP unicast routing
assigning IP addresses to Layer 3 interfaces 35-4
configuring static routes 35-5
disabling 35-4
enabling 35-4
inter-VLAN 35-1
IP addressing
classes 35-4
configuring 35-4
steps to configure 35-3
subnet mask 35-4
with SVIs 35-3
IPv4 ACLs
applying to interfaces 33-17
extended, creating 33-8
named 33-12
standard, creating 33-7
IPv4 and IPv6
dual protocol stacks 36-5
IPv6
ACLs
displaying 38-8
limitations 38-2
matching criteria 38-3

port 38-1
precedence 38-2
router 38-1
supported 38-2
addresses 36-2
address formats 36-2
applications 36-5
assigning address 36-8
autoconfiguration 36-5
configuring static routes 36-11
default configuration 36-7
defined 36-1
forwarding 36-8
ICMP 36-3
monitoring 36-12
neighbor discovery 36-3
SDM templates 37-1, 38-1
Stateless Autoconfiguration 36-5
supported features 36-2
IPv6 traffic, filtering 38-3

J

join messages, IGMP 23-3

L

LACP
See EtherChannel
Layer 2 frames, classification with CoS 34-2
Layer 2 interfaces, default configuration 13-11
Layer 2 traceroute
and ARP 40-15
and CDP 40-15
broadcast traffic 40-14
described 40-14
IP addresses and subnets 40-15
MAC addresses and VLANs 40-15
multicast traffic 40-15
multiple devices on a port 40-15
unicast traffic 40-14
usage guidelines 40-15
Layer 3 features 1-11
Layer 3 interfaces
assigning IP addresses to 35-4
assigning IPv6 addresses to 36-8
changing from Layer 2 mode 35-4
Layer 3 packets, classification methods 34-2
LDAP 4-2
Leaking IGMP Reports 20-4
LEDs, switch
See hardware installation guide
lightweight directory access protocol
See LDAP
line configuration mode 2-2
Link Aggregation Control Protocol
See EtherChannel
link failure, detecting unidirectional 18-7
Link Layer Discovery Protocol
See CDP
link local unicast addresses 36-3
link redundancy
See Flex Links
links, unidirectional 25-1
link-state tracking
configuring 39-19
described 39-17
LLDP
configuring 27-4
characteristics 27-6
default configuration 27-4
enabling 27-5
monitoring and maintaining 27-11
overview 27-1
supported TLVs 27-1
switch stack considerations 27-2
transmission timer and holdtime, setting 27-6

LLDP-MED
configuring
procedures 27-4
TLVs 27-7
monitoring and maintaining 27-11
overview 27-1, 27-2
supported TLVs 27-2
LLDP Media Endpoint Discovery
See LLDP-MED
local SPAN 28-2
location TLV 27-3, 27-7
login authentication
with RADIUS 11-30
with TACACS+ 11-14
login banners 5-11
log messages
See system message logging
Long-Reach Ethernet (LRE) technology 1-15
loop guard
described 19-9
enabling 19-15
support for 1-7
LRE profiles, considerations in switch clusters 8-13

M

MAB
See MAC authentication bypass
MAB inactivity timer
default setting 12-36
range 12-38
MAC/PHY configuration status TLV 27-2
MAC addresses
aging time 5-15
and VLAN association 5-14
building the address table 5-14
default configuration 5-15
disabling learning on a VLAN 5-23
discovering 5-24
displaying 5-23
displaying in the IP source binding table 21-20
dynamic
learning 5-14
removing 5-16
in ACLs 33-21
static
adding 5-20
allowing 5-22, 5-23
characteristics of 5-20
dropping 5-22
removing 5-21
MAC address learning 1-5
MAC address learning, disabling on a VLAN 5-23
MAC address notification, support for 1-11
MAC address-table move update
configuration guidelines 20-8
configuring 20-12
default configuration 20-8
description 20-6
monitoring 20-14
MAC address-to-VLAN mapping 14-24
MAC authentication bypass 12-37
configuring 12-58
overview 12-17
MAC extended access lists
applying to Layer 2 interfaces 33-22
configuring for QoS 34-46
creating 33-21
defined 33-21
for QoS classification 34-5
MACSec 7-2
magic packet 12-27
manageability features 1-5
management access
in-band
browser session 1-5
CLI session 1-5
device manager 1-5

SNMP 1-5
out-of-band console port connection 1-5
management address TLV 27-2
management options
CLI 2-1
clustering 1-2
CNS 4-1
Network Assistant 1-2
overview 1-4
management VLAN
considerations in switch clusters 8-7
discovery through different management VLANs 8-7
mapping tables for QoS
configuring
CoS-to-DSCP 34-56
DSCP 34-56
DSCP-to-CoS 34-59
DSCP-to-DSCP-mutation 34-60
IP-precedence-to-DSCP 34-57
policed-DSCP 34-58
described 34-10
marking
action with aggregate policers 34-54
described 34-3, 34-8
matching
IPv6 ACLs 38-3
matching, IPv4 ACLs 33-5
maximum aging time
MSTP 18-24
STP 17-21
maximum hop count, MSTP 18-24
maximum number of allowed devices, port-based authentication 12-38
MDA
configuration guidelines 12-13 to 12-14
described 1-8, 12-13
exceptions with authentication process 12-5
membership mode, VLAN port 14-3
member switch
automatic discovery 8-4
defined 8-2
managing 8-13
passwords 8-12
recovering from lost connectivity 40-11
requirements 8-3
See also candidate switch, cluster standby group, and standby command switch
memory consistency check errors
example 40-23
memory consistency check routines 1-4, 40-23
memory consistency integrity 1-4, 40-23
messages, to users through banners 5-11
MIBs
overview 31-1
SNMP interaction with 31-4
mirroring traffic for analysis 28-1
mismatches, autonegotiation 40-11
module number 13-7
monitoring
access groups 33-24
cables for unidirectional links 25-1
CDP 26-5
features 1-11
Flex Links 20-14
IGMP
filters 23-28
snooping 23-16, 37-12
interfaces 13-20
IP SLAs operations 32-6
IPv4 ACL configuration 33-24
IPv6 36-12
IPv6 ACL configuration 38-8
MAC address-table move update 20-14
multicast router interfaces 23-16, 37-12
MVR 23-22
network traffic for analysis with probe 28-2
port
blocking 24-20

protection 24-20
SFP status 13-21, 40-13
speed and duplex mode 13-13
traffic flowing among switches 29-1
traffic suppression 24-20
VLANs 14-13
VMPS 14-28
VTP 15-16
mrouter Port 20-3
mrouter port 20-5
MSTP
boundary ports
configuration guidelines 18-15
described 18-6
BPDU filtering
described 19-3
enabling 19-12
BPDU guard
described 19-2
enabling 19-11
CIST, described 18-3
CIST regional root 18-3
CIST root 18-5
configuration guidelines 18-14, 19-10
configuring
forward-delay time 18-23
hello time 18-23
link type for rapid convergence 18-25
maximum aging time 18-24
maximum hop count 18-24
MST region 18-15
neighbor type 18-25
path cost 18-20
port priority 18-19
root switch 18-17
secondary root switch 18-18
switch priority 18-22
CST
defined 18-3
operations between regions 18-4
default configuration 18-14
default optional feature configuration 19-9
displaying status 18-26
enabling the mode 18-15
EtherChannel guard
described 19-7
enabling 19-14
extended system ID
effects on root switch 18-17
effects on secondary root switch 18-18
unexpected behavior 18-17
IEEE 802.1s
implementation 18-6
port role naming change 18-6
terminology 18-5
instances supported 17-9
interface state, blocking to forwarding 19-2
interoperability and compatibility among modes 17-10
interoperability with IEEE 802.1D
described 18-8
restarting migration process 18-26
IST
defined 18-2
master 18-3
operations within a region 18-3
loop guard
described 19-9
enabling 19-15
mapping VLANs to MST instance 18-16
MST region
CIST 18-3
configuring 18-15
described 18-2
hop-count mechanism 18-5
IST 18-2
supported spanning-tree instances 18-2
optional features supported 1-6

overview 18-2
Port Fast
described 19-2
enabling 19-10
preventing root switch selection 19-8
root guard
described 19-8
enabling 19-15
root switch
configuring 18-17
effects of extended system ID 18-17
unexpected behavior 18-17
shutdown Port Fast-enabled port 19-2
status, displaying 18-26
multiauth
support for inaccessible authentication bypass 12-25
multiauth mode
See multiple-authentication mode
multicast groups
Immediate Leave 23-5
joining 23-3
leaving 23-5
static joins 23-9, 37-8
multicast router interfaces, monitoring 23-16, 37-12
multicast router ports, adding 23-9, 37-8
multicast storm 24-1
multicast storm-control command 24-4
multicast television application 23-17
multicast VLAN 23-17
Multicast VLAN Registration
See MVR
multidomain authentication
See MDA
multiple authentication 12-14
multiple authentication mode
configuring 12-45
MVR
and address aliasing 23-20
and IGMPv3 23-20
configuration guidelines 23-20
configuring interfaces 23-21
default configuration 23-19
described 23-17
example application 23-17
modes 23-21
monitoring 23-22
multicast television application 23-17
setting global parameters 23-20
support for 1-4

N

NAC
critical authentication 12-24, 12-55
IEEE 802.1x authentication using a RADIUS server 12-60
IEEE 802.1x validation using RADIUS server 12-60
inaccessible authentication bypass 12-55
Layer 2 IEEE 802.1x validation 12-30, 12-60
named IPv4 ACLs 33-12
NameSpace Mapper
See NSM
native VLAN
configuring 14-19
default 14-19
NDAC 7-2
NEAT
configuring 12-61
overview 12-31
neighbor discovery, IPv6 36-3
Network Assistant
benefits 1-1
described 1-4
downloading image files 1-2
guide mode 1-2
management options 1-2
managing switch stacks 9-2, 9-13
upgrading a switch 42-24

wizards 1-2
network configuration examples
increasing network performance 1-14
long-distance, high-bandwidth transport 1-16
providing network services 1-15
server aggregation and Linux server cluster 1-15
small to medium-sized network 1-16
network design
performance 1-14
services 1-15
Network Device Admission Control (NDAC) 7-2
Network Edge Access Topology
See NEAT
network management
CDP 26-1
RMON 29-1
SNMP 31-1
network performance, measuring with IP SLAs 32-2
network policy TLV 27-2, 27-7
Network Time Protocol
See NTP
no commands 2-4
nonhierarchical policy maps
described 34-9
non-IP traffic filtering 33-21
nontrunking mode 14-14
normal-range VLANs 14-4
configuration guidelines 14-6
configuring 14-4
defined 14-1
NSM 4-3
NTP
associations
defined 5-2
overview 5-2
stratum 5-2
support for 1-5
time
services 5-2
synchronizing 5-2

O

offline configuration for switch stacks 9-6
off mode, VTP 15-3
online diagnostics
overview 41-1
running tests 41-3
understanding 41-1
open1x
configuring 12-66
open1x authentication
overview 12-30
optimizing system resources 10-1
options, management 1-4
out-of-profile markdown 1-10

P

packet modification, with QoS 34-16
PAgP
See EtherChannel
passwords
default configuration 11-2
disabling recovery of 11-5
encrypting 11-3
for security 1-8
in clusters 8-12
overview 11-1
recovery of 40-3
setting
enable 11-3
enable secret 11-3
Telnet 11-6
with usernames 11-7
VTP domain 15-8
path cost

MSTP 18-20
STP 17-18
PC (passive command switch) 8-9
performance, network design 1-14
performance features 1-3
persistent self-signed certificate 11-47
per-user ACLs and Filter-Ids 12-8
per-VLAN spanning-tree plus
See PVST+
physical ports 13-2
PIM-DVMRP, as snooping method 23-8
ping
character output description 40-14
executing 40-13
overview 40-13
PoE
auto mode 13-5
CDP with power consumption, described 13-4
CDP with power negotiation, described 13-4
Cisco intelligent power management 13-4
configuring 13-16
devices supported 13-4
high-power devices operating in low-power mode 13-4
IEEE power classification levels 13-5
power budgeting 13-17
power consumption 13-17
powered-device detection and initial power allocation 13-4
power management modes 13-5
power negotiation extensions to CDP 13-4
standards supported 13-4
static mode 13-6
troubleshooting 40-12
policed-DSCP map for QoS 34-58
policers
configuring
for each matched traffic class 34-49
for more than one traffic class 34-54
described 34-3
displaying 34-74
number of 34-35
types of 34-9
policing
described 34-3
token-bucket algorithm 34-9
policy maps for QoS
characteristics of 34-49
described 34-7
displaying 34-75
nonhierarchical on physical ports
described 34-9
port ACLs
defined 33-2
types of 33-2
Port Aggregation Protocol
See EtherChannel
port-based authentication
accounting 12-16
authentication server
defined 6-2, 12-3
RADIUS server 12-3
client, defined 6-2, 12-3
configuration guidelines 6-9, 12-36
configuring
802.1x authentication 12-42
guest VLAN 12-53
host mode 12-45
inaccessible authentication bypass 12-55
manual re-authentication of a client 12-48
periodic re-authentication 12-47
quiet period 12-48
RADIUS server 6-13, 12-45
RADIUS server parameters on the switch 6-11, 12-43
restricted VLAN 12-53
switch-to-client frame-retransmission number 12-49, 12-50

switch-to-client retransmission time 12-48
violation modes 12-41
default configuration 6-9, 12-35
described 12-1
device roles 6-2, 12-2
displaying statistics 6-17, 12-68
downloadable ACLs and redirect URLs
configuring 12-63 to 12-65, ?? to 12-65
overview 12-20 to 12-22
EAPOL-start frame 12-5
EAP-request/identity frame 12-5
EAP-response/identity frame 12-5
enabling
802.1X authentication 6-11
encapsulation 12-3
flexible authentication ordering
configuring 12-65
overview 12-30
guest VLAN
configuration guidelines 12-23, 12-24
described 12-22
host mode 12-11
inaccessible authentication bypass
configuring 12-55
described 12-24
guidelines 12-37
initiation and message exchange 12-5
magic packet 12-27
maximum number of allowed devices per port 12-38
method lists 12-42
multiple authentication 12-14
per-user ACLs
configuration tasks 12-20
described 12-19
RADIUS server attributes 12-19
ports
authorization state and dot1x port-control command 12-10
authorized and unauthorized 12-10
voice VLAN 12-26
port security
described 12-27
readiness check
configuring 12-38
described 12-17, 12-38
resetting to default values 12-67
statistics, displaying 12-68
switch
as proxy 6-2, 12-3
RADIUS client 12-3
switch supplicant
configuring 12-61
overview 12-31
user distribution
guidelines 12-29
overview 12-29
VLAN assignment
AAA authorization 12-42
characteristics 12-18
configuration tasks 12-18
described 12-17
voice aware 802.1x security
configuring 12-39
described 12-31, 12-39
voice VLAN
described 12-26
PVID 12-26
VVID 12-26
wake-on-LAN, described 12-27
with ACLs and RADIUS Filter-Id attribute 12-33
port-based authentication methods, supported 12-7
port blocking 1-3, 24-7
port-channel
See EtherChannel
port description TLV 27-1
Port Fast
described 19-2
enabling 19-10

mode, spanning tree 14-25
support for 1-6
port membership modes, VLAN 14-3
port priority
MSTP 18-19
STP 17-16
ports
access 13-2
blocking 24-7
dynamic access 14-4
protected 24-6
static-access 14-3, 14-10
switch 13-2
trunks 14-3, 14-14
VLAN assignments 14-10
port security
aging 24-17
and QoS trusted boundary 34-39
configuring 24-12
default configuration 24-11
described 24-8
displaying 24-20
on trunk ports 24-14
sticky learning 24-9
violations 24-10
with other features 24-11
port-shutdown response, VMPS 14-24
port VLAN ID TLV 27-2
power management TLV 27-2, 27-7
Power over Ethernet
See PoE
preemption, default configuration 20-8
preemption delay, default configuration 20-8
preferential treatment of traffic
See QoS
preventing unauthorized access 11-1
primary links 20-2
priority
overriding CoS 16-6
trusting CoS 16-6
private VLAN edge ports
See protected ports
privileged EXEC mode 2-2
privilege levels
changing the default for lines 11-9
command switch 8-14
exiting 11-10
logging into 11-10
mapping on member switches 8-14
overview 11-2, 11-8
setting a command with 11-8
protected ports 1-8, 24-6
protocol storm protection 24-18
provisioning new members for a switch stack 9-6
proxy reports 20-3
pruning, VTP
disabling
in VTP domain 15-14
on a port 14-19
enabling
in VTP domain 15-14
on a port 14-19
examples 15-6
overview 15-5
pruning-eligible list
changing 14-19
for VTP pruning 15-5
VLANs 15-14
PVST+
described 17-9
IEEE 802.1Q trunking interoperability 17-10
instances supported 17-9

Q

QoS
and MQC commands 34-1
auto-QoS

categorizing traffic 34-17
configuration and defaults display 34-31
configuration guidelines 34-29
described 34-16
disabling 34-31
displaying generated commands 34-31
displaying the initial configuration 34-31
effects on running configuration 34-29
list of generated commands 34-20, 34-24
basic model 34-3
classification
class maps, described 34-7
defined 34-3
DSCP transparency, described 34-40
flowchart 34-6
forwarding treatment 34-2
in frames and packets 34-2
IP ACLs, described 34-7
MAC ACLs, described 34-5, 34-7
options for IP traffic 34-5
options for non-IP traffic 34-4
policy maps, described 34-7
trust DSCP, described 34-4
trusted CoS, described 34-4
trust IP precedence, described 34-4
class maps
configuring 34-47
displaying 34-74
configuration guidelines
auto-QoS 34-29
standard QoS 34-34
configuring
aggregate policers 34-54
auto-QoS 34-16
default port CoS value 34-38
DSCP maps 34-56
DSCP transparency 34-40
DSCP trust states bordering another domain 34-41
egress queue characteristics 34-66
ingress queue characteristics 34-62
IP extended ACLs 34-45
IP standard ACLs 34-43
MAC ACLs 34-46
port trust states within the domain 34-36
trusted boundary 34-39
default auto configuration 34-17
default standard configuration 34-32
displaying statistics 34-74
DSCP transparency 34-40
egress queues
allocating buffer space 34-67
buffer allocation scheme, described 34-14
configuring shaped weights for SRR 34-71
configuring shared weights for SRR 34-72
described 34-3
displaying the threshold map 34-70
flowchart 34-14
mapping DSCP or CoS values 34-69
scheduling, described 34-4
setting WTD thresholds 34-67
WTD, described 34-15
enabling globally 34-36
flowcharts
classification 34-6
egress queueing and scheduling 34-14
ingress queueing and scheduling 34-12
policing and marking 34-10
implicit deny 34-7
ingress queues
allocating bandwidth 34-64
allocating buffer space 34-64
buffer and bandwidth allocation, described 34-13
configuring shared weights for SRR 34-64
configuring the priority queue 34-65
described 34-3
displaying the threshold map 34-63
flowchart 34-12

mapping DSCP or CoS values 34-62
priority queue, described 34-13
scheduling, described 34-3
setting WTD thresholds 34-62
WTD, described 34-13
IP phones
automatic classification and queueing 34-17
detection and trusted settings 34-17, 34-39
limiting bandwidth on egress interface 34-73
mapping tables
CoS-to-DSCP 34-56
displaying 34-74
DSCP-to-CoS 34-59
DSCP-to-DSCP-mutation 34-60
IP-precedence-to-DSCP 34-57
policed-DSCP 34-58
types of 34-10
marked-down actions 34-51
marking, described 34-3, 34-8
overview 34-1
packet modification 34-16
policers
configuring 34-51, 34-54
described 34-8
displaying 34-74
number of 34-35
types of 34-9
policies, attaching to an interface 34-8
policing
described 34-3, 34-8
token bucket algorithm 34-9
policy maps
characteristics of 34-49
displaying 34-75
nonhierarchical on physical ports 34-49
QoS label, defined 34-3
queues
configuring egress characteristics 34-66
configuring ingress characteristics 34-62
high priority (expedite) 34-15, 34-73
location of 34-11
SRR, described 34-12
WTD, described 34-11
rewrites 34-16
support for 1-10
trust states
bordering another domain 34-41
described 34-4
trusted device 34-39
within the domain 34-36
quality of service
See QoS
queries, IGMP 23-4
query solicitation, IGMP 23-12

R

RADIUS
attributes
vendor-proprietary 11-38
vendor-specific 11-36
configuring
accounting 11-35
authentication 11-30
authorization 11-34
communication, global 11-28, 11-36
communication, per-server 11-28
multiple UDP ports 11-28
default configuration 11-27
defining AAA server groups 11-32
displaying the configuration 11-40
identifying the server 11-28
in clusters 8-13
limiting the services to the user 11-34
method list, defined 11-26
operation of 11-19
overview 11-18
server load balancing 11-40

suggested network environments 11-18
tracking services accessed by user 11-35
RADIUS Change of Authorization 11-20
range
macro 13-9
of interfaces 13-8
rapid convergence 18-9
rapid per-VLAN spanning-tree plus
See rapid PVST+
rapid PVST+
described 17-9
IEEE 802.1Q trunking interoperability 17-10
instances supported 17-9
Rapid Spanning Tree Protocol
See RSTP
rcommand command 8-13
RCP
configuration files
downloading 42-17
overview 42-16
preparing the server 42-16
uploading 42-18
image files
deleting old image 42-36
downloading 42-34
preparing the server 42-33
uploading 42-36
readiness check
port-based authentication
configuring 12-38
described 12-17, 12-38
reconfirmation interval, VMPS, changing 14-27
reconfirming dynamic VLAN membership 14-27
recovery procedures 40-1
redirect URL 12-20, 12-21, 12-63
redundancy
EtherChannel 39-3
STP
backbone 17-8
path cost 14-22
port priority 14-20
redundant links and UplinkFast 19-13
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 23-6
disabling 23-15, 37-11
resequencing ACL entries 33-12
reserved addresses in DHCP pools 21-22
resetting a UDLD-shutdown interface 25-6
responder, IP SLAs
described 32-3
enabling 32-5
response time, measuring with IP SLAs 32-4
restricted VLAN
configuring 12-53
described 12-23
using with IEEE 802.1x 12-23
restricting access
overview 11-1
passwords and privilege levels 11-2
RADIUS 11-18
TACACS+ 11-10
retry count, VMPS, changing 14-28
RFC
1112, IP multicast and IGMP 23-2
1157, SNMPv1 31-2
1166, IP addresses 35-4
1305, NTP 5-2
1757, RMON 29-2

1901, SNMPv2C 31-2
1902 to 1907, SNMPv2 31-2
2236, IP multicast and IGMP 23-2
2273-2275, SNMPv3 31-2
RFC 5176 Compliance 11-21
RMON
default configuration 29-3
displaying status 29-6
enabling alarms and events 29-3
groups supported 29-2
overview 29-1
statistics
collecting group Ethernet 29-6
collecting group history 29-5
support for 1-11
root guard
described 19-8
enabling 19-15
support for 1-7
root switch
MSTP 18-17
STP 17-14
router ACLs
defined 33-2
types of 33-3
RSPAN
characteristics 28-7
configuration guidelines 28-15
default configuration 28-9
defined 28-2
destination ports 28-6
displaying status 28-21
interaction with other features 28-8
monitored ports 28-5
monitoring ports 28-6
overview 1-11, 28-1
received traffic 28-4
sessions
creating 28-15
defined 28-3
limiting source traffic to specific VLANs 28-20
specifying monitored ports 28-15
with ingress traffic enabled 28-19
source ports 28-5
transmitted traffic 28-5
VLAN-based 28-6
RSTP
active topology 18-9
BPDU
format 18-12
processing 18-12
designated port, defined 18-9
designated switch, defined 18-9
interoperability with IEEE 802.1D
described 18-8
restarting migration process 18-26
topology changes 18-13
overview 18-8
port roles
described 18-9
synchronized 18-11
proposal-agreement handshake process 18-10
rapid convergence
described 18-9
edge ports and Port Fast 18-9
point-to-point links 18-10, 18-25
root ports 18-10
root port, defined 18-9
See also MSTP
running configuration
replacing 42-19, 42-20
rolling back 42-19, 42-21
running configuration, saving 3-15

S

SC (standby command switch) 8-9
scheduled reloads 3-23

SCP
and SSH 11-52
configuring 11-53
SDM
templates
configuring 10-2
number of 10-1
SDM template 38-3
configuration guidelines 10-1
configuring 10-1
types of 10-1
Secure Copy Protocol
secure HTTP client
configuring 11-51
displaying 11-52
secure HTTP server
configuring 11-50
displaying 11-52
secure MAC addresses
deleting 24-16
maximum number of 24-9
types of 24-9
secure remote connections 11-42
Secure Shell
See SSH
Secure Socket Layer
See SSL
security, port 24-8
Security Exchange Protocol (SXP) 7-2
security features 1-7
Security Group Access Control List (SGACL) 7-2
Security Group Tag (SGT) 7-2
See SCP
sequence numbers in log messages 30-7
server mode, VTP 15-3
service-provider network, MSTP and RSTP 18-1
set-request operation 31-4
setup program
failed command switch replacement 40-10
replacing failed command switch 40-8
severity levels, defining in system messages 30-8
SFPs
monitoring status of 13-21, 40-13
security and identification 40-12
status, displaying 40-13
SGACL 7-2
SGT 7-2
shaped round robin
See SRR
show access-lists hw-summary command 33-18
show and more command output, filtering 2-9
show cdp traffic command 26-5
show cluster members command 8-13
show configuration command 13-18
show forward command 40-21
show interfaces command 13-13, 13-18
show interfaces switchport 20-4
show lldp traffic command 27-11
show platform forward command 40-21
show platform tcam command 40-23
show running-config command
displaying ACLs 33-17, 33-18
interface description in 13-18
shutdown command on interfaces 13-22
Simple Network Management Protocol
See SNMP
small-frame arrival rate, configuring 24-5
SNAP 26-1
SNMP
accessing MIB variables with 31-4
agent
described 31-4
disabling 31-9
and IP SLAs 32-2
authentication level 31-12
community strings
configuring 31-9
for cluster switches 31-4

overview 31-4
configuration examples 31-19
default configuration 31-8
engine ID 31-8
groups 31-8, 31-11
host 31-8
ifIndex values 31-5
in-band management 1-5
in clusters 8-13
informs
and trap keyword 31-14
described 31-5
differences from traps 31-5
disabling 31-17
enabling 31-17
limiting access by TFTP servers 31-18
limiting system log messages to NMS 30-9
manager functions 1-4, 31-3
managing clusters with 8-14
notifications 31-5
overview 31-1, 31-4
security levels 31-3
setting CPU threshold notification 31-17
status, displaying 31-20
system contact and location 31-18
trap manager, configuring 31-15
traps
described 31-3, 31-5
differences from informs 31-5
disabling 31-17
enabling 31-14
enabling MAC address notification 5-16, 5-18, 5-19
overview 31-1, 31-4
types of 31-14
users 31-8, 31-11
versions supported 31-2
SNMP and Syslog Over IPv6 36-6
SNMPv1 31-2
SNMPv2C 31-2
SNMPv3 31-2
snooping, IGMP 23-1
software compatibility
See stacks, switch
software images
location in flash 42-24
recovery procedures 40-2
scheduling reloads 3-23
tar file format, described 42-25
See also downloading and uploading
source addresses
in IPv4 ACLs 33-9
in IPv6 ACLs 38-5
source-and-destination-IP address based forwarding, EtherChannel 39-7
source-and-destination MAC address forwarding, EtherChannel 39-7
source-IP address based forwarding, EtherChannel 39-7
source-MAC address forwarding, EtherChannel 39-6
SPAN
configuration guidelines 28-10
default configuration 28-9
destination ports 28-6
displaying status 28-21
interaction with other features 28-8
monitored ports 28-5
monitoring ports 28-6
overview 1-11, 28-1
ports, restrictions 24-12
received traffic 28-4
sessions
configuring ingress forwarding 28-13, 28-20
creating 28-10
defined 28-3
limiting source traffic to specific VLANs 28-14
removing destination (monitoring) ports 28-12
specifying monitored ports 28-10
with ingress traffic enabled 28-12

source ports 28-5
transmitted traffic 28-5
VLAN-based 28-6
spanning tree and native VLANs 14-15
Spanning Tree Protocol
See STP
SPAN traffic 28-4
SRR
configuring
shaped weights on egress queues 34-71
shared weights on egress queues 34-72
shared weights on ingress queues 34-64
described 34-12
shaped mode 34-12
shared mode 34-12
support for 1-10, 1-11
SSH
configuring 11-43
cryptographic software image 11-41
described 1-5, 11-42
encryption methods 11-42
switch stack considerations 9-14
user authentication methods, supported 11-42
SSL
configuration guidelines 11-49
configuring a secure HTTP client 11-51
configuring a secure HTTP server 11-50
cryptographic software image 11-46
described 11-46
monitoring 11-52
stack, switch
MAC address of 9-5, 9-16
stack changes, effects on
IP routing 35-3
stack master
bridge ID (MAC address) 9-5
defined 9-1
election 9-4
See also stacks, switch
stack member
accessing CLI of specific member 9-21
configuring
member number 9-19
priority value 9-20
defined 9-1
displaying information of 9-22
number 9-5
priority value 9-6
provisioning a new member 9-20
replacing 9-13
See also stacks, switch
stack protocol version 9-9
stacks, switch
accessing CLI of specific member 9-21
assigning information
member number 9-19
priority value 9-20
provisioning a new member 9-20
auto-advise 9-10
auto-copy 9-10
auto-extract 9-10
auto-upgrade 9-10
bridge ID 9-5
compatibility, software 9-8
configuration file 9-13
configuration scenarios 9-14
default configuration 9-16
description of 9-1
displaying information of 9-22
enabling persistent MAC address timer 9-16
incompatible software and image upgrades 9-12
management connectivity 9-13
managing 9-1
membership 9-2
merged 9-3
MSTP instances supported 17-9
offline configuration
described 9-6

effects of adding a provisioned switch 9-7
effects of removing a provisioned switch 9-8
effects of replacing a provisioned switch 9-8
provisioned configuration, defined 9-6
provisioned switch, defined 9-6
provisioning a new member 9-20
partitioned 9-3
provisioned switch
adding 9-7
removing 9-8
replacing 9-8
replacing a failed member 9-13
software compatibility 9-8
software image version 9-8
stack protocol version 9-9
system-wide configuration considerations 9-13
version-mismatch (VM) mode
automatic upgrades with auto-upgrade 9-10
examples 9-11
manual upgrades with auto-advise 9-10
upgrades with auto-extract 9-10
version-mismatch mode
described 9-9
See also stack master and stack member
standby command switch
configuring
considerations 8-10
defined 8-2
priority 8-9
requirements 8-3
virtual IP address 8-10
See also cluster standby group and HSRP
standby group, cluster
See cluster standby group and HSRP
standby links 20-2
startup configuration
booting
manually 3-19
specific image 3-20
clearing 42-19
configuration file
automatically downloading 3-18
specifying the filename 3-18
static access ports
assigning to VLAN 14-10
defined 13-2, 14-3
static addresses
See addresses
static MAC addressing 1-8
static routes
configuring 35-5
configuring for IPv6 36-11
static VLAN membership 14-2
statistics
802.1X 6-17
802.1x 12-68
CDP 26-5
interface 13-21
LLDP 27-11
LLDP-MED 27-11
NMSP 27-11
QoS ingress and egress 34-74
RMON group Ethernet 29-6
RMON group history 29-5
SNMP input and output 31-20
VTP 15-16
sticky learning 24-9
storm control
configuring 24-3
described 24-1
disabling 24-5
displaying 24-20
support for 1-3
thresholds 24-1
STP
accelerating root port selection 19-4
BackboneFast
described 19-5

disabling 19-14
enabling 19-13
BPDU filtering
described 19-3
disabling 19-12
enabling 19-12
BPDU guard
described 19-2
disabling 19-12
enabling 19-11
BPDU message exchange 17-3
configuration guidelines 17-12, 19-10
configuring
forward-delay time 17-21
hello time 17-20
maximum aging time 17-21
path cost 17-18
port priority 17-16
root switch 17-14
secondary root switch 17-16
spanning-tree mode 17-13
switch priority 17-19
transmit hold-count 17-22
counters, clearing 17-22
default configuration 17-11
default optional feature configuration 19-9
designated port, defined 17-3
designated switch, defined 17-3
detecting indirect link failures 19-5
disabling 17-14
displaying status 17-22
EtherChannel guard
described 19-7
disabling 19-14
enabling 19-14
extended system ID
effects on root switch 17-14
effects on the secondary root switch 17-16
overview 17-4
unexpected behavior 17-14
features supported 1-6
IEEE 802.1D and bridge ID 17-4
IEEE 802.1D and multicast addresses 17-8
IEEE 802.1t and VLAN identifier 17-4
inferior BPDU 17-3
instances supported 17-9
interface state, blocking to forwarding 19-2
interface states
blocking 17-5
disabled 17-7
forwarding 17-5, 17-6
learning 17-6
listening 17-6
overview 17-4
interoperability and compatibility among modes 17-10
limitations with IEEE 802.1Q trunks 17-10
load sharing
overview 14-20
using path costs 14-22
using port priorities 14-20
loop guard
described 19-9
enabling 19-15
modes supported 17-9
multicast addresses, effect of 17-8
optional features supported 1-6
overview 17-2
path costs 14-22
Port Fast
described 19-2
enabling 19-10
port priorities 14-21
preventing root switch selection 19-8
protocols supported 17-9
redundant connectivity 17-8
root guard
described 19-8

enabling 19-15
root port, defined 17-3
root switch
configuring 17-14
effects of extended system ID 17-4, 17-14
election 17-3
unexpected behavior 17-14
shutdown Port Fast-enabled port 19-2
status, displaying 17-22
superior BPDU 17-3
timers, described 17-20
UplinkFast
described 19-4
enabling 19-13
stratum, NTP 5-2
subnet mask 35-4
success response, VMPS 14-24
summer time 5-7
SunNet Manager 1-4
supported port-based authentication methods 12-7
SVIs
and IP unicast routing 35-3
and router ACLs 33-3
connecting VLANs 13-6
defined 13-3
switch 36-2
switch clustering technology 8-1
See also clusters, switch
switch console port 1-5
Switch Database Management
See SDM
Switched Port Analyzer
See SPAN
switched ports 13-2
switchport backup interface 20-4, 20-5
switchport block multicast command 24-8
switchport block unicast command 24-8
switchport protected command 24-7
switch priority
MSTP 18-22
STP 17-19
switch software features 1-1
switch virtual interface
See SVI
SXP 7-2
syslog
See system message logging
system capabilities TLV 27-2
system clock
configuring
daylight saving time 5-7
manually 5-5
summer time 5-7
time zones 5-6
displaying the time and date 5-5
overview 5-1
See also NTP
system description TLV 27-2
system message logging
default configuration 30-3
defining error message severity levels 30-8
disabling 30-3
displaying the configuration 30-13
enabling 30-4
facility keywords, described 30-13
level keywords, described 30-9
limiting messages 30-9
message format 30-2
overview 30-1
sequence numbers, enabling and disabling 30-7
setting the display destination device 30-4
synchronizing log messages 30-5
syslog facility 1-11
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 name
default configuration 5-9
default setting 5-9
manual configuration 5-9
See also DNS
system name TLV 27-2
system prompt, default setting 5-8, 5-9
system resources, optimizing 10-1

T

TACACS+
accounting, defined 11-12
authentication, defined 11-11
authorization, defined 11-11
configuring
accounting 11-17
authentication key 11-13
authorization 11-16
login authentication 11-14
default configuration 11-13
displaying the configuration 11-18
identifying the server 11-13
in clusters 8-13
limiting the services to the user 11-16
operation of 11-12
overview 11-10
support for 1-9
tracking services accessed by user 11-17
tar files
creating 42-6
displaying the contents of 42-6
extracting 42-7
image file format 42-25
TCAM
memory consistency check errors
example 40-23
memory consistency check routines 1-4, 40-23
memory consistency integrity 1-4, 40-23
space
HFTM 40-23
HQATM 40-23
unassigned 40-23
TDR 1-11
Telnet
accessing management interfaces 2-9
number of connections 1-5
setting a password 11-6
temporary self-signed certificate 11-47
Terminal Access Controller Access Control System Plus
See TACACS+
terminal lines, setting a password 11-6
ternary content addressable memory
See TCAM
TFTP
configuration files
downloading 42-11
preparing the server 42-10
uploading 42-12
configuration files in base directory 3-7
configuring for autoconfiguration 3-7
image files
deleting 42-28
downloading 42-26
preparing the server 42-26
uploading 42-28
limiting access by servers 31-18
TFTP server 1-5
threshold, traffic level 24-2
time
See NTP and system clock
Time Domain Reflector
See TDR
time-range command 33-14
time ranges in ACLs 33-14
time stamps in log messages 30-7
time zones 5-6
TLVs

defined 27-1
LLDP 27-1
LLDP-MED 27-2
Token Ring VLANs
support for 14-5
VTP support 15-4
ToS 1-10
traceroute, Layer 2
and ARP 40-15
and CDP 40-15
broadcast traffic 40-14
described 40-14
IP addresses and subnets 40-15
MAC addresses and VLANs 40-15
multicast traffic 40-15
multiple devices on a port 40-15
unicast traffic 40-14
usage guidelines 40-15
traceroute command 40-17
See also IP traceroute
traffic
blocking flooded 24-8
fragmented 33-4
fragmented IPv6 38-2
unfragmented 33-4
traffic policing 1-10
traffic suppression 24-1
transmit hold-count
see STP
transparent mode, VTP 15-3
trap-door mechanism 3-2
traps
configuring MAC address notification 5-16, 5-18, 5-19
configuring managers 31-14
defined 31-3
enabling 5-16, 5-18, 5-19, 31-14
notification types 31-14
overview 31-1, 31-4
troubleshooting
connectivity problems 40-13, 40-14, 40-16
CPU utilization 40-24
detecting unidirectional links 25-1
displaying crash information 40-22
setting packet forwarding 40-21
SFP security and identification 40-12
show forward command 40-21
with CiscoWorks 31-4
with debug commands 40-18
with ping 40-13
with system message logging 30-1
with traceroute 40-16
trunk failover
See link-state tracking
trunking encapsulation 1-7
trunk ports
configuring 14-16
defined 13-3, 14-3
trunks
allowed-VLAN list 14-17
load sharing
setting STP path costs 14-22
using STP port priorities 14-20, 14-21
native VLAN for untagged traffic 14-19
parallel 14-22
pruning-eligible list 14-19
to non-DTP device 14-14
trusted boundary for QoS 34-39
trusted port states
between QoS domains 34-41
classification options 34-4
ensuring port security for IP phones 34-39
support for 1-10
within a QoS domain 34-36
trustpoints, CA 11-46
twisted-pair Ethernet, detecting unidirectional links 25-1
type of service
See ToS

U

UDLD
- configuration guidelines 25-4
- default configuration 25-4
- disabling
  - globally 25-5
  - on fiber-optic interfaces 25-5
  - per interface 25-5
- echoing detection mechanism 25-2
- enabling
  - globally 25-4
  - per interface 25-5
- link-detection mechanism 25-1
- neighbor database 25-2
- overview 25-1
- resetting an interface 25-6
- status, displaying 25-6
- support for 1-6

unauthorized ports with IEEE 802.1x 12-10
unicast MAC address filtering 1-5
- and adding static addresses 5-21
- and broadcast MAC addresses 5-21
- and CPU packets 5-21
- and multicast addresses 5-21
- and router MAC addresses 5-21
- configuration guidelines 5-21
- described 5-21

unicast storm 24-1
unicast storm control command 24-4
unicast traffic, blocking 24-8
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 15-4
upgrading software images
- See downloading

UplinkFast
- described 19-4
- disabling 19-13
- enabling 19-13

uploading
- configuration files
  - preparing 42-10, 42-13, 42-16
  - reasons for 42-8
  - using FTP 42-15
  - using RCP 42-18
  - using TFTP 42-12
- image files
  - preparing 42-26, 42-29, 42-33
  - reasons for 42-24
  - using FTP 42-32
  - using RCP 42-36
  - using TFTP 42-28

user EXEC mode 2-2
username-based authentication 11-7

V

version-dependent transparent mode 15-4
version-mismatch (VM) mode
- automatic upgrades with auto-upgrade 9-10
- manual upgrades with auto-advise 9-10
- upgrades with auto-extract 9-10

version-mismatch mode
- described 9-9

virtual IP address
- cluster standby group 8-10
- command switch 8-10

virtual switches and PAgP 39-4
vlan.dat file 14-4
VLAN 1, disabling on a trunk port 14-17
VLAN 1 minimization 14-17
vlan-assignment response, VMPS 14-24
VLAN configuration

at bootup 14-7
saving 14-7
VLAN configuration mode 2-2
VLAN database
and startup configuration file 14-7
and VTP 15-1
VLAN configuration saved in 14-6
VLANs saved in 14-4
VLAN filtering and SPAN 28-6
vlan global configuration command 14-6
VLAN ID, discovering 5-24
VLAN load balancing on flex links 20-2
configuration guidelines 20-8
VLAN management domain 15-2
VLAN Management Policy Server
See VMPS
VLAN membership
confirming 14-27
modes 14-3
VLAN Query Protocol
See VQP
VLANs
adding 14-8
adding to VLAN database 14-8
aging dynamic addresses 17-9
allowed on trunk 14-17
and spanning-tree instances 14-3, 14-6, 14-12
configuration guidelines, extended-range VLANs 14-11
configuration guidelines, normal-range VLANs 14-6
configuring 14-1
configuring IDs 1006 to 4094 14-11
connecting through SVIs 13-6
creating 14-9
default configuration 14-8
deleting 14-9
described 13-1, 14-1
displaying 14-13
extended-range 14-1, 14-11
features 1-7
illustrated 14-2
limiting source traffic with RSPAN 28-20
limiting source traffic with SPAN 28-14
modifying 14-8
multicast 23-17
native, configuring 14-19
normal-range 14-1, 14-4
parameters 14-5
port membership modes 14-3
static-access ports 14-10
STP and IEEE 802.1Q trunks 17-10
supported 14-3
Token Ring 14-5
traffic between 14-2
VTP modes 15-3
VLAN Trunking Protocol
See VTP
VLAN trunks 14-14
VMPS
administering 14-28
configuration example 14-29
configuration guidelines 14-25
default configuration 14-25
description 14-23
dynamic port membership
described 14-24
reconfirming 14-27
troubleshooting 14-29
entering server address 14-26
mapping MAC addresses to VLANs 14-24
monitoring 14-28
reconfirmation interval, changing 14-27
reconfirming membership 14-27
retry count, changing 14-28
voice aware 802.1x security
port-based authentication
configuring 12-39
described 12-31, 12-39

voice-over-IP 16-1
voice VLAN
Cisco 7960 phone, port connections 16-1
configuration guidelines 16-3
configuring IP phones for data traffic
override CoS of incoming frame 16-6
trust CoS priority of incoming frame 16-6
configuring ports for voice traffic in
802.1p priority tagged frames 16-5
802.1Q frames 16-4
connecting to an IP phone 16-4
default configuration 16-3
described 16-1
displaying 16-6
IP phone data traffic, described 16-2
IP phone voice traffic, described 16-2
VQP 1-7, 14-23
VTP
adding a client to a domain 15-15
advertisements 14-15, 15-3
and extended-range VLANs 14-3, 15-1
and normal-range VLANs 14-3, 15-1
client mode, configuring 15-11
configuration
guidelines 15-8
requirements 15-10
saving 15-8
configuration requirements 15-10
configuration revision number
guideline 15-15
resetting 15-16
consistency checks 15-4
default configuration 15-7
described 15-1
domain names 15-8
domains 15-2
modes
client 15-3
off 15-3
server 15-3
transitions 15-3
transparent 15-3
monitoring 15-16
passwords 15-8
pruning
disabling 15-14
enabling 15-14
examples 15-6
overview 15-5
support for 1-7
pruning-eligible list, changing 14-19
server mode, configuring 15-10, 15-13
statistics 15-16
support for 1-7
Token Ring support 15-4
transparent mode, configuring 15-10
using 15-1
Version
enabling 15-13
version, guidelines 15-9
Version 1 15-4
Version 2
configuration guidelines 15-9
overview 15-4
Version 3
overview 15-4

W

web authentication 12-17
configuring 6-16 to ??
described 1-7
web-based authentication
customizeable web pages 6-6
description 6-1
web-based authentication, interactions with other features 6-7
weighted tail drop

See WTD
wired location service
configuring 27-9
displaying 27-11
location TLV 27-3
understanding 27-3
wizards 1-2
WTD
described 34-11
setting thresholds
egress queue-sets 34-67
ingress queues 34-62
support for 1-10, 1-11

X

Xmodem protocol 40-2