INDEX

ACLs
applying IPv6 ACLs to a Layer 3 interface 39-22

Numerics

10/100 autonegotiation feature, forced 6-11
10-Gigabit Ethernet or Gigabit Ethernet ports
deploy on WS-X4606-10GE-E and Sup 6-E 6-7
10-Gigabit Ethernet port
deploy with Gigabit Ethernet SFP ports 6-6
1400 W DC Power supply
special considerations 10-16
1400 W DC SP Triple Input power supply
special considerations 10-17
802.10 SAID (default) 13-4
802.1Q
trunks 17-6
tunneling
compatibility with other features 22-5
defaults 22-4
described 22-2
tunnel ports with other features 22-6
802.1Q VLANs
encapsulation 15-3
trunk restrictions 15-5
802.1s
See MST
802.1w
See MST
802.1X
See port-based authentication
802.1X authentication
for Critical Authentication 34-12
for guest VLANs 34-8
for MAC Authentication Bypass 34-9
for Wake-on-LAN 34-12
RADIUS accounting 34-16
with port security 34-15
with VLAN assignment 34-7
with voice VLAN ports 34-18
802.3ad
See LACP

A

AAA 36-1
abbreviating commands 2-5
access control entries
See ACEs
access control entries and lists 36-1
access-group mode, configuring on Layer 2 interface 39-35
access-group mode, using PACL with 39-35
access list filtering, SPAN enhancement 43-13
access lists
using with WCCP 49-7
access ports
and Layer 2 protocol tunneling 22-9
configure port security 35-6, 35-21
configuring 15-8
access VLANs 15-6
accounting
configuring for 802.1X 34-32
with TACACS+ 3-16, 3-21
ACEs

ACLs 39-2
IP 39-2
Layer 4 operation restrictions 39-15
ACEs and ACLs 36-1
ACLs
ACEs 39-2
and SPAN 43-5
and TCAM programming for Sup 6-E 39-15
and TCAM programming for Sup II-Plus thru V-10GE 39-6
applying on routed packets 39-32
applying on switched packets 39-31
chaning the TCAM programming algorithm 39-9
compatibility on the same switch 39-3
configuring with VLAN maps 39-31
CPU impact 39-17
hardware and software support 39-5
IP, matching criteria for port ACLs 39-4
MAC extended 39-19
matching criteria for router ACLs 39-3
port
and voice VLAN 39-4
defined 39-3
limitations 39-5
processing 39-17
resize the TCAM regions 39-10
selecting mode of capturing control packets 39-12
TCAM programming algorithm 39-7
troubleshooting high CPU 39-12
types supported 39-3
understanding 39-2
VLAN maps 39-5
ACLs and VLAN maps, examples 39-25
acronyms, list of A-1
action drivers, marking 32-75
active queue management 32-14
active queue management via DBL, QoS on Sup 6-E 32-85
adding members to a community 12-8
addresses
displaying the MAC address table 4-30
dynamic
changing the aging time 4-21
defined 4-19
learning 4-20
removing 4-22
MAC, discovering 4-30
See MAC addresses
static
adding and removing 4-27
defined 4-19
address resolution 4-30
adjacency tables
description 27-2
displaying statistics 27-9
advertisements, VTP
See VTP advertisements
aggregation switch, enabling DHCP snooping 37-9
aging time
MAC address table 4-21
applying IPv6 ACLs to a Layer 3 interface 39-22
AQM via DBL, QoS on Sup 6-E 32-85
ARP
defined 4-30
table
address resolution 4-30
managing 4-30
asymmetrical links, and 802.1Q tunneling 22-4
audience xxxvii
authentication
NTP associations 4-4
See also port-based authentication
TACACS+
defined 3-16
key 3-18
login 3-19
Authentication, Authorization, and Accounting (AAA) 36-1

Authentication Failed VLAN assignment
configure with 802.1X 34-40
authentication server
defined 34-3
RADIUS server 34-3
authoritative time source, described 4-2
authorization
with TACACS+ 3-16, 3-21
authorized and unauthorized ports 34-4
authorized ports with 802.1X 34-4
autoconfiguration 3-2
automatic discovery
considerations 12-7
automatic QoS
See QoS
Auto-MDIX on a port
configuring 6-20
displaying the configuration 6-21
overview 6-19
autonegotiation feature
forced 10/100Mbps 6-11
Auto-QoS
configuring 32-17
auto-sync command 8-8

B

Baby Giants
interacting with 6-19
BackboneFast
adding a switch (figure) 18-3
and MST 17-23
configuring 18-16
link failure (figure) 18-14, 18-15
not supported MST 17-23
understanding 18-13
See also STP
banners
configuring
login 4-19
message-of-the-day login 4-18
default configuration 4-18
when displayed 4-17
b command 51-3
b flash command 51-3
BGP 1-7
routing session with multi-VRF CE 31-7
blocking packets 41-1
blocking state (STP)
RSTP comparisons (table) 17-24
boot bootldr command 3-31
boot command 3-28
boot commands 51-3
boot fields
See configuration register boot fields
bootstrap program
See ROM monitor
boot system command 3-26, 3-31
boot system flash command 3-28
Border Gateway Protocol
See BGP
boundary ports
description 17-27
BPDU Guard
and MST 17-23
configuring 18-16
overview 18-8
BPDUs
and media speed 17-2
pseudobridges and 17-25
what they contain 17-3
bridge ID
See STP bridge ID
bridge priority (STP) 17-16
bridge protocol data units
See BPDUs
Broadcast Storm Control
disabling 42-6

enabling 42-3
BSR
configuration example 29-21
burst rate 32-56
burst size 32-31

C

cache engine clusters xxxix, 49-1
cache engines xxxix, 49-1
cache farms
See cache engine clusters
candidates
automatic discovery 12-7
candidate switch, cluster
defined 12-12
requirements 12-12
Capturing control packets
selecting mode 39-12
cautions
Unicast RPF
BGP optional attributes 28-4
cautions for passwords
encrypting 3-22
CDP
and trusted boundary 32-26
automatic discovery in communities 12-7
configuration 23-2
displaying configuration 23-3
enabling on interfaces 23-3
Layer 2 protocol tunneling 22-7
maintaining 23-3
monitoring 23-3
overview 1-2, 23-1
cdp enable command 23-3
CEF
adjacency tables 27-2
and NSF with SSO 9-5
configuring load balancing 27-7
displaying statistics 27-8
enabling 27-6
hardware switching 27-4
load balancing 27-6
overview 27-1
software switching 27-4
CGMP
overview 20-1
channel-group group command 19-7, 19-10
Cisco 7600 series Internet router
enabling SNMP 50-16
Cisco Discovery Protocol
See CDP
Cisco Express Forwarding
See CEF
Cisco Group Management Protocol
See CGMP
Cisco IOS NSF-aware
support 9-2
Cisco IOS NSF-capable support 9-2
Cisco IP Phones
configuring 33-2
sound quality 33-1
CiscoWorks 2000 45-4
CIST
description 17-22
class-map command 32-33
class of service
See CoS
clear cdp counters command 23-4
clear cdp table command 23-3
clear counters command 6-23
clearing
IP multicast table entries 29-20
clear ip eigrp neighbors command 26-18
clear ip flow stats command 46-9
CLI
accessing 2-1
backing out one level 2-5

getting commands 2-5
history substitution 2-3
managing clusters 12-12
modes 2-5
monitoring environments 43-1
ROM monitor 2-7
software basics 2-4
clients
in 802.1X authentication 34-2
clock
See system clock
clustering switches
command switch characteristics 12-11, 12-12
and VTY 12-11
convert to a community 12-9
managing
through CLI 12-12
overview 12-10
planning considerations
CLI 12-12
passwords 12-8
command-line processing 2-3
command modes 2-5
commands
b 51-3
b flash 51-3
boot 51-3
confreg 51-3
dev 51-3
dir device 51-3
frame 51-5
i 51-3
listing 2-5
meminfo 51-5
reset 51-3
ROM monitor 51-2 to 51-3
ROM monitor debugging 51-5
SNMP 50-16
sysret 51-5
command switch, cluster
requirements 12-11
common and internal spanning tree
See CIST
common spanning tree
See CST
community of switches
access modes in Network Assistant 12-8
adding devices 12-8
candidate characterisitcs 12-6
communication protocols 12-8
community name 12-7
configuration information 12-8
converting from a cluster 12-9
host name 12-7
passwords 12-8
community ports 40-4
community strings
configuring 45-7
overview 45-4
community VLANs 40-3, 40-4
and SPAN features 40-12
configure as a PVLAN 40-13
compiling MIBs 50-16
config-register command 3-29
config terminal command 3-9
configurable leave timer,IGMP 20-3
configuration examples
SNMP 45-16
configuration files
limiting TFTP server access 45-15
obtaining with DHCP 3-6
saving 3-10
system contact and location information 45-15
configuration guidelines
SNMP 45-6
configuration register
boot fields
listing value 3-29

modifying 3-28
changing from ROM monitor 51-3
changing settings 3-28 to 3-29
configuring 3-26
settings at startup 3-27
configure terminal command 3-28, 6-2
configuring access-group mode on Layer 2 interface 39-35
configuring flow control 6-14
configuring interface link and trunk status envents 6-24
configuring named IPv6 ACLs 39-20
configuring named MAC extended ACLs 39-19
configuring unicast MAC address filtering 39-19
configuring VLAN maps 39-23
confreg command 51-3
console configuration mode 2-5
console download 51-4 to 51-5
console port
disconnecting user sessions 7-6
monitoring user sessions 7-6
control plane policing
See CoPP
CoPP
applying QoS service policy to control plane 36-3
configuring
ACLs to match traffic 36-3
enabling MLS QoS 36-3
packet classification criteria 36-3
service-policy map 36-3
control plane configuration mode
entering 36-3
displaying
dynamic information 36-7
number of conforming bytes and packets 36-7
rate information 36-7
entering control plane configuration mode 36-3
monitoring statistics 36-7
overview 36-1
copy running-config startup-config command 3-10
copy system:running-config nvram:startup-config command 3-31
CoS
definition 32-3
figure 32-2
overriding on Cisco IP Phones 33-4
priority 33-4
CoS Mutation
configuring 32-40
CoS-to-DSCP maps 32-57
CoS value, configuring for an interface 32-53
counters
clearing MFIB 29-21
clearing on interfaces 6-23
CPU, impact of ACL processing 39-17
CPU port sniffing 43-10
Critical Authentication
configure with 802.1X 34-36, 34-37
CST
description 17-25
IST and 17-22
MST and 17-22
customer edge devices 31-2

D

database agent
configuration examples 37-12
enabling the DHCP Snooping 37-12
daylight saving time 4-13
debug commands, ROM monitor 51-5
default configuration
802.1X 34-22
auto-QoS 32-17
banners 4-18
DNS 4-16
IGMP filtering 20-18
IGMP snooping 21-5, 21-6
Layer 2 protocol tunneling 22-9

MAC address table 4-21
multi-VRF CE 31-4
NTP 4-4
private VLANs 40-11
resetting the interface 6-26
RMON 47-3
SNMP 45-6
SPAN and RSPAN 43-6
system message logging 44-3
system name and prompt 4-15
TACACS+ 3-18
default gateway
configuring 3-11
verifying configuration 3-11
default settings, erase commad 3-31
denial-of-service attacks
IP address spoofing, mitigating 28-5
Unicast RPF, deploying 28-5
denying access to a server on another VLAN 39-29
deploying 10-Gigabit Ethernet and a Gigabit Ethernet SFP ports 6-6
deploying 10-Gigabit Ethernet and a Gigabit Ethernet SFP ports on WS-X4606-10GE-E and Sup 6-E 6-7
description command 6-13
detecting unidirectional links 24-1
dev command 51-3
DHCP-based autoconfiguration
client request message exchange 3-3
configuring
client side 3-2
DNS 3-5
relay device 3-5
server-side 3-3
TFTP server 3-4
example 3-7
lease options
for IP address information 3-3
for receiving the configuration file 3-4
overview 3-2
relationship to BOOTP 3-2
DHCP option 82
overview 37-3
DHCP Snooping
enabling, and Option 82 37-9
DHCP snooping
accepting untrusted packets form edge switch 37-10
configuring 37-6
default configuration 37-7
displaying binding tables 37-16
displaying configuration 37-16
displaying information 37-15
enabling 37-7
enabling on private VLAN 37-11
enabling on the aggregation switch 37-9
enabling the database agent 37-12
message exchange process 37-4
monitoring 37-20
option 82 data insertion 37-3
overview 37-1
Snooping database agent 37-2
DHCP Snooping Database Agent
adding to the database (example) 37-15
enabling (example) 37-12
overview 37-2
reading from a TFTP file (example) 37-14
Diagnostics
online 48-1
troubleshooting 48-2
Power-On-Self-Test
causes of failure 48-14
how it works 48-3
overview 48-3
Power-On-Self-Test for Supervisor Engine V-10GE 48-8
Differentiated Services Code Point values
See DSCP values
DiffServ architecture, QoS 32-2
Digital optical monitoring transceiver support 6-10

dir device command 51-3
disabled state
RSTP comparisons (table) 17-24
disabling
broadcast storm control 42-6
disabling multicast storm control 42-7
disconnect command 7-6
discovery, clusters
See automatic discovery
displaying storm control 42-7
DNS
and DHCP-based autoconfiguration 3-5
default configuration 4-16
displaying the configuration 4-17
overview 4-15
setting up 4-16
documentation
organization xxxvii
related xl
domain names
DNS 4-15
Domain Name System
See DNS
double-tagged packets
802.1Q tunneling 22-2
Layer 2 protocol tunneling 22-9
downloading MIBs 50-14, 50-15
drop threshold for Layer 2 protocol packets 22-10
DSCP maps 32-57
DSCP-to-CoS maps
configuring 32-59
DSCP values
configuring maps 32-57
definition 32-4
IP precedence 32-2
mapping markdown 32-24
mapping to transmit queues 32-55
DSCP values, configuring port value 32-54
DTP
VLAN trunks and 15-3
duplex command 6-12
duplex mode
configuring interface 6-11
dynamic ARP inspection
ARP cache poisoning 38-2
configuring
ACLs for non-DHCP environments 38-11
in DHCP environments 38-5
log buffer 38-14
rate limit for incoming ARP packets 38-16
denial-of-service attacks, preventing 38-16
interface trust state, security coverage 38-3
log buffer
configuring 38-14
logging of dropped packets 38-4
overview 38-1
port channels, their behavior 38-5
priority of static bindings 38-4
purpose of 38-2
rate limiting of ARP packets 38-4
configuring 38-16
validation checks, performing 38-19
dynamic buffer limiting
globally 32-27
on specific CoS values 32-29
on specific IP DSCP values 32-28
Dynamic Host Configuration Protocol snooping
See DHCP snooping
dynamic port VLAN membership
example 13-25
limit on hosts 13-24
reconfirming 13-22
troubleshooting 13-24
Dynamic Trunking Protocol
See DTP

E

EAP frames
- changing retransmission time 34-45
- exchanging (figure) 34-4, 34-6, 34-11
- request/identity 34-3
- response/identity 34-3
- setting retransmission number 34-46

EAPOL frames
- 802.1X authentication and 34-3
- OTP authentication, example (figure) 34-4, 34-11
- start 34-3

edge ports
- description 17-27

EGP
- overview 1-7

EIGRP
- configuration examples 26-19
- monitoring and maintaining 26-18

EIGRP (Enhanced IGRP)
- stub routing
  - benefits 26-17
  - configuration tasks 26-17
  - configuring 26-13
  - overview 26-13
  - restrictions 26-17
  - verifying 26-18

EIGRP (enhanced IGRP)
- overview 1-8

eigrp stub command 26-18

EIGRP stub routing, configuring 26-12

Embedded CiscoView
- displaying information 4-33
- installing and configuring 4-31
- overview 4-31

emergency alarms on Sup Engine 6-E systems 10-3

enable command 3-9, 3-28

enable mode 2-5

enabling or disabling QOS on an interface 32-50

enabling SNMP 50-16

encapsulation types 15-3

Enhanced Interior Gateway Routing Protocol
- See EIGRP

environmental conditions
- Sup Engine 6-E 10-2
- Sup Engines II-Plus to V-10GE 10-2

environmental monitoring
- using CLI commands 10-1

EtherChannel
- channel-group group command 19-7, 19-10
- configuration guidelines 19-5
- configuring 19-6 to 19-14
- configuring Layer 2 19-9
- configuring Layer 3 19-6
- interface port-channel command 19-7
- lacp system-priority
  - command example 19-12
- modes 19-3
- overview 19-1
- PAgP
  - Understanding 19-3
- physical interface configuration 19-7
- port-channel interfaces 19-2
- port-channel load-balance command 19-13
- removing 19-14
- removing interfaces 19-14

EtherChannel guard
- disabling 18-6
- enabling 18-6
- overview 18-6

explicit host tracking
- enabling 20-10

extended range VLANs
- See VLANs

Extensible Authentication Protocol over LAN 34-1

Exterior Gateway Protocol
- See EGP

F

FastDrop
- clearing entries 29-20
- displaying entries 29-19
- overview 29-10

FIB
- description 27-2
- See also MFIB

filtering
- in a VLAN 39-23
- non-IP traffic 39-19

flags 29-11

Flash memory
- configuring router to boot from 3-30
- loading system images from 3-30
- security precautions 3-30

flooded traffic, blocking 41-2

flowchart, traffic marking procedure 32-75

flow control, configuring 6-14

forward-delay time (STP)
- configuring 17-18

forwarding information base
- See FIB

frame command 51-5

G

gateway
- See default gateway

get-bulk-request operation 45-3

get-next-request operation 45-3, 45-4

get-request operation 45-3, 45-4

get-response operation 45-3

Gigabit Ethernet SFP ports
- deploy with 10-Gigabit Ethernet 6-6

global configuration mode 2-5

Guest-VLANs
- configure with 802.1X 34-32, 34-41

H

hardware and software ACL support 39-5

hardware switching 27-5

hello time (STP)
- configuring 17-17

hierarchical policers, configuring 32-46

hierarchical policies, QoS on Sup 6-E 32-87

high CPU due to ACLs, troubleshooting 39-12

history
- CLI 2-3

history table, level and number of syslog messages 44-9

hop counts
- configuring MST bridges 17-28

host
- configuring host statically 20-10
- limit on dynamic port 13-24

host ports
- kinds of 40-4

Hot Standby Routing Protocol
- See HSRP

HSRP
- description 1-7

http
- //www.cisco.com/en/US/docs/ios/fundamentals/command reference/cf_book.html 44-1, 47-1

hw-module module num power command 10-20

I

ICMP
- enabling 7-11
- ping 7-7
- running IP traceroute 7-8
- time exceeded messages 7-8

i command 51-3

IDS
- using with SPAN and RSPAN 43-2

IEEE 802.1s

See MST
IEEE 802.1w
See MST
IEEE 802.3ad
See LACP
IGMP
configurable leave timer
enabling 20-8
configurable-leave timer 20-3
description 29-3
enabling 29-13
explicit host tracking 20-4, 20-10
immediate-leave processing 20-3
leave processing, enabling 21-8
overview 20-1
report suppression
disabling 21-11
IGMP filtering
configuring 20-18
default configuration 20-18
described 20-18
monitoring 20-21
IGMP groups
setting the maximum number 20-20
IGMP Immediate Leave
configuration guidelines 20-8
IGMP profile
applying 20-19
configuration mode 20-18
configuring 20-19
IGMP snooping
configuration guidelines 20-4
default configuration 21-5, 21-6
enabling 20-5, 20-6
enabling and disabling 21-6
IP multicast and 29-4
monitoring 20-13, 21-11
overview 20-1
IGRP
description 1-8
Immediate Leave, IGMP
enabling 21-8
immediate-leave processing
enabling 20-8
IGMP
See fast-leave processing
ingress packets, SPAN enhancement 43-12
inline power
configuring on Cisco IP phones 33-5
insufficient inline power handling for Supervisor Engine II-TS 10-18
Intelligent Power Management 11-4
interacting with Baby Giants 6-19
interface command 3-9, 6-1
interface link and trunk status events
configuring 6-24
interface port-channel command 19-7
interface range command 6-4
interface range macro command 6-5
interfaces
adding descriptive name 6-13
clearing counters 6-23
configuring 6-2
configuring ranges 6-4
displaying information about 6-23
Layer 2 modes 15-4
maintaining 6-22
monitoring 6-22
naming 6-13
numbers 6-2
overview 6-1
restarting 6-24
See also Layer 2 interfaces
Interior Gateway Routing Protocol
See IGRP
Internet Control Message Protocol
See ICMP
Internet Group Management Protocol

See IGMP
Inter-Switch Link encapsulation
See ISL encapsulation
Intrusion Detection System
See IDS
IP
configuring default gateway 3-11
configuring static routes 3-11
displaying statistics 27-8
flow switching cache 46-9
IP addresses
cluster candidate or member 12-12
cluster command switch 12-11
discovering 4-30
ip cef command 27-6
IP Enhanced IGRP
interfaces, displaying 26-18
ip flow-aggregation cache destination-prefix command 46-11
ip flow-aggregation cache prefix command 46-11
ip flow-aggregation cache source-prefix command 46-12
ip flow-export command 46-9
ip icmp rate-limit unreachable command 7-12
ip igmp profile command 20-18
ip igmp snooping tcn flood command 20-12
ip igmp snooping tcn flood query count command 20-12
ip igmp snooping tcn query solicit command 20-13
IP information
assigned
through DHCP-based autoconfiguration 3-2
ip load-sharing per-destination command 27-7
ip local policy route-map command 30-5
ip mask-reply command 7-13
IP MTU sizes, configuring 26-8
IP MTU sizes,configuring 26-8
IP multicast
clearing table entries 29-20
configuring 29-12
default configuration 29-13
displaying PIM information 29-16
displaying the routing table information 29-16
enabling 29-13
enabling dense-mode PIM 29-14
enabling sparse-mode 29-14
features not supported 29-12
hardware forwarding 29-8
IGMP snooping and 20-4, 29-4
monitoring 29-15
overview 29-1
routing protocols 29-2
software forwarding 29-8
See also Auto-RP; IGMP; PIM; RP; RPF
ip multicast-routing command 29-13
IP phones
automatic classification and queueing 32-17
configuring voice ports 33-3
See Cisco IP Phones 33-1
trusted boundary for QoS 32-26
ip pim command 29-14
ip pim dense-mode command 29-14
ip pim sparse-dense-mode command 29-15
ip policy route-map command 30-4
IP Port Security for Static Hosts
on a Layer 2 access port 37-21
on a PVLAN host port 37-24
overview 37-21
ip redirects command 7-12
ip route-cache flow command 46-7
IP routing tables
deleting entries 29-20
IP Source Guard
configuring 37-17
configuring on private VLANs 37-19
displaying 37-19, 37-20
overview 37-16
IP statistics
displaying 27-8
IP traceroute

executing 7-8
overview 7-8
IP unicast
displaying statistics 27-8
IP Unnumbered support
configuring on a range of Ethernet VLANs 14-5
configuring on LAN and VLAN interfaces 14-4
configuring with connected host polling 14-6
DHCP Option 82 14-2
displaying settings 14-7
format of agent remote ID suboptions 14-3
troubleshooting 14-8
with conected host polling 14-3
with DHCP server and Relay agent 14-2
ip unreachables command 7-11
IPX
redistribution of route information with EIGRP 1-8
ISL
encapsulation 15-3
trunking with 802.1Q tunneling 22-4
isolated port 40-4
isolated VLANs 40-3, 40-4
ISSU
compatibility matrix 5-13
compatiblity verification using Cisco Feature Navigator 5-14
NSF overview 5-4
perform the process
aborting a software upgrade 5-26
configuring the rollback timer as a safeguard 5-27
displaying a compatibility matrix 5-29
loading the new software on the new standby 5-24
stopping the rollback timer 5-23
switching to the standby 5-20
verify the ISSU state 5-16
verify the redundancy mode 5-15
verify the software installation 5-14
vload the new software on standby 5-17
prerequisites 5-2
process overview 5-7
restrictions 5-2
SNMP support 5-13
SSO overview 5-4
versioning capability in software to support 5-12
IST
and MST regions 17-22
description 17-22
master 17-27

J

jumbo frames
and ethernet ports 6-18
configuring MTU sizes for 6-18
ports and linecards that support 6-16
understanding MTUs 6-17
understanding support 6-17
VLAN interfaces 6-18

K

keyboard shortcuts 2-3

L

l2protocol-tunnel command 22-11
labels, definition 32-3
LACP
system ID 19-4
Layer 2 access ports 15-8
Layer 2 Control Packet QoS
feature interaction 32-64
overview 32-60
usage guidelines 32-64
Layer 2 frames
classification with CoS 32-2

Layer 2 interface, configuring access-mode mode on 39-35
Layer 2 interfaces
assigning VLANs 13-7
configuring 15-5
configuring as PVLAN host ports 40-16
configuring as PVLAN promiscuous ports 40-15
configuring as PVLAN trunk ports 40-17
defaults 15-5
disabling configuration 15-9
modes 15-4
show interfaces command 15-7
Layer 2 interface type
resetting 40-22
setting 40-22
Layer 2 protocol tunneling
default configuration 22-9
guidelines 22-10
Layer 2 switching
overview 15-1
Layer 2 Traceroute
and ARP 7-10
and CDP 7-9
host-to-host paths 7-9
IP addresses and subnets 7-10
MAC addresses and VLANs 7-10
multicast traffic 7-10
multiple devices on a port 7-10
unicast traffic 1-20, 7-9
usage guidelines 7-9
Layer 2 trunks
configuring 15-6
overview 15-3
Layer 3 interface, applying IPv6 ACLs 39-22
Layer 3 interface counters,configuring 26-10
Layer 3 interface counters,understanding 26-4
Layer 3 interfaces
configuration guidelines 26-5
overview 26-1
logical 26-2
physical 26-2
VLANs as interfaces 26-7
Layer 3 packets
classification methods 32-2
Layer 4 port operations
configuration guidelines 39-16
restrictions 39-15
limitations on using a TwinGig Convertor 6-8
link and trunk status events
configuring interface 6-24
listening state (STP)
RSTP comparisons (table) 17-24
load balancing
configuring for CEF 27-7
configuring for EtherChannel 19-13
overview 19-4, 27-6
per-destination 27-7
Logical Layer 3 interfaces
configuring 26-5
login authentication
with TACACS+ 3-19
login banners 4-17
login timer
changing 7-5
logoutwarning command 7-6
loop guard
and MST 17-23
configuring 18-4
overview 18-3

M

MAC addresses
aging time 4-21
allocating 17-5
and VLAN association 4-20
building tables 4-20, 15-2
convert dynamic to sticky secure 35-5

default configuration 4-21
discovering 4-30
displaying 4-30, 7-3
displaying in DHCP snooping binding table 37-16
dynamic
learning 4-20
removing 4-22
in ACLs 39-19
static
adding 4-28
allowing 4-29
characteristics of 4-27
dropping 4-29
removing 4-28
sticky 35-4
sticky secure, adding 35-5
MAC Authentication Bypass
configure with 802.1X 34-35
MAC extended access lists 39-19
macros
See Smartports macros
main-cpu command 8-8
management options
SNMP 45-1
mapping
DSCP markdown values 32-24
DSCP values to transmit queues 32-55
mapping tables
configuring DSCP 32-57
described 32-14
marking
hardware capabilities 32-77
marking action drivers 32-75
marking network traffic 32-72
marking support, multi-attribute 32-76
mask destination command 46-11
mask source command 46-11, 46-12
Match CoS for non-IPV4 traffic
configuring 32-35
match ip address command 30-3
maximum aging time (STP)
configuring 17-18
MDA
configuration guidelines 34-19 to 34-20
described 34-19
members
automatic discovery 12-7
member switch
managing 12-12
member switch, cluster
defined 12-11
requirements 12-12
meminfo command 51-5
messages, to users through banners 4-17
metro tags 22-2
MFIB
CEF 29-5
displaying 29-18
overview 29-11
MIBs
compiling 50-16
downloading 50-14, 50-15
overview 45-1
related information 50-15
SNMP interaction with 45-4
MLD Done messages and Immediate-leave 21-4
MLD messages 21-2
MLD queries 21-3
MLD reports 21-4
MLD Snooping
MLD Done messages and Immediate-leave 21-4
MLD messages 21-2
MLD queries 21-3
MLD reports 21-4
Multicast client aging robustness 21-3
Multicast router discovery 21-3
overview 21-1
Mode of capturing control packets, selecting 39-12

modules
checking status 7-1
powering down 10-20
monitoring
802.1Q tunneling 22-12
ACL information 39-39
IGMP
snooping 21-11
IGMP filters 20-21
IGMP snooping 20-13
Layer 2 protocol tunneling 22-12
multicast router interfaces 21-11
multi-VRF CE 31-12
traffic flowing among switches 47-1
tunneling 22-12
VLAN filters 39-30
VLAN maps 39-30
M-record 17-23
MST
and multiple spanning trees 1-3, 17-22
boundary ports 17-27
BPDUs 17-23
configuration parameters 17-26
configuring 17-29
displaying configurations 17-33
edge ports 17-27
enabling 17-29
hop count 17-28
instances
configuring parameters 17-32
description 17-22
number supported 17-26
interoperability with PVST+ 17-23
link type 17-28
master 17-27
message age 17-28
regions 17-26
restrictions 17-29
to-SST interoperability 17-24
MSTP
EtherChannel guard
enabling 18-6
M-record 17-23
M-tree 17-23
M-tree 17-23
MTUS
understanding 6-17
MTU size
configuring 6-18, 6-25
default 13-4
multicast
See IP multicast
Multicast client aging robustness 21-3
multicast groups
static joins 21-7
multicast packets
blocking 41-2
Multicast router discovery 21-3
multicast router interfaces, monitoring 21-11
multicast router ports, adding 21-8
multicast routers
displaying routing tables 29-16
flood suppression 20-10
Multicast Storm Control
enabling 42-4
disabling 42-7
suppression on Sup 6-E 42-4
suppression on WS-X4014 42-5
suppression on WS-X4016 42-5
WS-X4515, WS-X4014, and WS-X4013+ Sup Engs 42-5
WS-X4516 Sup Eng 42-5
multidomain authentication
See MDA
Multiple Domain Authentication
configuring 34-28
overview of Host Mode 34-6

multiple forwarding paths 1-3, 17-22
Multiple Spanning Tree
See MST
multiple VPN routing/forwarding
See multi-VRF CE
multi-VRF CE
components 31-4
configuration example 31-8
default configuration 31-4
defined 31-1
displaying 31-12
monitoring 31-12
network components 31-4
packet-forwarding process 31-4

N

named aggregate policers, creating 32-31
named IPv6 ACLs, configuring
ACLs
configuring named IPv6 ACLs 39-20
named MAC extended ACLs
ACLs
configuring named MAC extended 39-19
native VLAN
and 802.1Q tunneling 22-4
specifying 15-6
NetFlow
aggregation
minimum mask,default value 46-11
destination-prefix aggregation
configuration (example) 46-16
minimum mask, configuring 46-11
IP
flow switching cache 46-9
prefix aggregation
configuration (example) 46-14
minimum mask, configuring 46-11
source-prefix aggregation
minimum mask, configuring 46-11
switching
checking for required hardware 46-6
configuration (example) 46-13
configuring switched IP flows 46-8
enabling Collection 46-7
exporting cache entries 46-9
statistics 46-9
NetFlow statistics
caveats on supervisor 46-6
checking for required hardware 46-6
configuring collection 46-6
enabling Collection 46-7
exporting cache entries 46-9
overview of collection 46-1
switched/bridged IP flows 46-8
Network Assistant
and VTY 12-11
configure
enable communication with switch 12-13, 12-17
default configuration 12-2
overview of CLI commands 12-2
network fault tolerance 1-3, 17-22
network management
configuring 23-1
RMON 47-1
SNMP 45-1
Network Time Protocol
See NTP
network traffic, marking 32-72
New Software Features in Release 7.7
TDR 7-3
Next Hop Resolution Protocol
See NHRP
NFFC/NFFC II
IGMP snooping and 20-4
NHRP
support 1-8
non-IP traffic filtering 39-19

non-RPF traffic
description 29-9
in redundant configurations (figure) 29-10
Nonstop Forwarding
See NSF
nonvolatile random-access memory
See NVRAM
normal-range VLANs
See VLANs
NSF
defined 9-1
guidelines and restrictions 9-9
operation 9-4
NSF-aware
supervisor engines 9-3
support 9-2
NSF-capable
supervisor engines 9-3
support 9-2
NSF with SSO supervisor engine redundancy
and CEF 9-5
overview 9-3
SSO operation 9-4
NTP
associations
authenticating 4-4
defined 4-2
enabling broadcast messages 4-7
peer 4-6
server 4-6
default configuration 4-4
displaying the configuration 4-11
overview 4-2
restricting access
creating an access group 4-9
disabling NTP services per interface 4-10
source IP address, configuring 4-10
stratum 4-2
synchronizing devices 4-6
time
services 4-2
synchronizing 4-2
NVRAM
saving settings 3-10

O

OIR
overview 6-22
Online Diagnostics 48-1
online insertion and removal
See OIR
Open Shortest Path First
See OSPF
operating system images
See system images
Option 82
enabling DHCP Snooping 37-9
OSPF
area concept 1-9
description 1-9

P

packets
modifying 32-16
software processed
and QoS 32-16
packet type filtering
overview 43-15
SPAN enhancement 43-15
PACL, using with access-group mode 39-35
PACL with VLAN maps and router ACLs 39-37
PAgP
understanding 19-3
passwords
configuring enable password 3-13

configuring enable secret password 3-13
encrypting 3-22
in clusters 12-8
recovering lost enable password 3-25
setting line password 3-14
PBR (policy-based routing)
configuration (example) 30-5
enabling 30-3
features 30-2
overview 30-1
route maps 30-2
when to use 30-2
per-port and VLAN Access Control List 37-16
per-port per-VLAN QoS
enabling 32-48
overview 32-16
Per-VLAN Rapid Spanning Tree 17-6
enabling 17-20
overview 17-6
PE to CE routing, configuring 31-7
Physical Layer 3 interfaces, configuring 26-11
PIM
configuring dense mode 29-14
configuring sparse mode 29-14
displaying information 29-15
displaying statistics 29-20
enabling sparse-dense mode 29-14, 29-15
overview 29-3
PIM-DM 29-3
PIM-SM 29-3
ping
executing 7-7
overview 7-7
ping command 7-7, 29-16
PoE 11-7
configuring power consumption for single device 11-5
configuring power consumption for switch 11-4
power consumption for powered devices
Intelligent Power Management 11-4
powering down a module 10-20
power management modes 11-2
show interface status 11-6
point-to-point
in 802.1X authentication (figure) 34-2, 34-17
police command 32-37
policed-DSCP map 32-58
policers
description 32-5
types of 32-10
policies
See QoS policies
policing
how to implement 32-72
See QoS policing
policy associations, QoS on Sup 6-E 32-89
policy-map command 32-33, 32-36
policy map marking action, configuring 32-77
policy maps
attaching to interfaces 32-40
configuring 32-35
port ACLs
and voice VLAN 39-4
defined 39-3
limitations 39-5
Port Aggregation Protocol
see PAgP
port-based authentication
802.1X with voice VLAN 34-18
changing the quiet period 34-44
client, defined 34-2
configuration guidelines 34-23
configure 802.1X accounting 34-32
configure switch-to-RADIUS server communication 34-26
configure with Authentication Failed VLAN assignment 34-40
configure with Critical Authentication 34-36, 34-37

configure with Guest-VLANs 34-32, 34-41
configure with MAC Authentication Bypass 34-35
configure with Wake-on-LAN 34-39
configuring
Multiple Domain Authentication 34-28
configuring Guest-VLAN 34-26
configuring manual re-authentication of a client 34-47
controlling authorization state 34-4
default configuration 34-22
described 34-1
device roles 34-2
displaying statistics 34-48
enabling 34-23
enabling multiple hosts 34-43
enabling periodic re-authentication 34-42
encapsulation 34-3
host mode 34-6
initiation and message exchange 34-3
method lists 34-23
multidomain authentication 34-19
multiple-hosts mode, described 34-6
port security
multiple-hosts mode 34-7
ports not supported 34-4
resetting to default values 34-48
setting retransmission number 34-46
setting retransmission time 34-45
topologies, supported 34-21
using with port security 34-15
with Critical Authentication 34-12
with Guest VLANs 34-8
with MAC Authentication Bypass 34-9
with VLAN assignment 34-7
port-based QoS features
See QoS
port-channel interfaces
See also EtherChannel
creating 19-6
overview 19-2
port-channel load-balance
command 19-12
command example 19-12
port-channel load-balance command 19-13
port cost (STP)
configuring 17-15
PortFast
and MST 17-23
BPDU filter, configuring 18-9
configuring or enabling 18-16
overview 18-6
PortFast BPDU filtering
and MST 17-23
enabling 18-9
overview 18-9
port numbering with TwinGig Convertors 6-8
port priority
configuring MST instances 17-32
configuring STP 17-13
ports
blocking 41-1
checking status 7-2
dynamic VLAN membership
example 13-25
reconfirming 13-22
forwarding, resuming 41-3
See also interfaces
port security
aging 35-5
and QoS trusted boundary 32-26
configuring 35-7
displaying 35-26
guidelines and restrictions 35-31
on access ports 35-6, 35-21
on private VLAN 35-13
host 35-14
over Layer 2 EtherChannel 35-31
promiscuous 35-15

topology 35-14, 35-17, 35-31
on trunk port 35-16
guidelines and restrictions 35-14, 35-17, 35-20, 35-31
port mode changes 35-21
on voice ports 35-21
RADIUS accounting 34-16
sticky learning 35-5
using with 802.1X 34-15
violations 35-5
with 802.1X Authentication 35-30
with DHCP and IP Source Guard 35-30
with other features 35-31
port states
description 17-5
port trust state
See trust states
power
inline 33-5
power dc input command 10-17
power handling for Supervisor Engine II-TS 11-11
power inline command 11-3
power inline consumption command 11-4, 11-5
power management
Catalyst 4500 series 10-6
Catalyst 4500 Switch power supplies 10-13
Catalyst 4948 series 10-20
configuring combined mode 10-12
configuring redundant mode 10-11
overview 10-1
redundancy 10-6
power management for Catalyst 4500 Switch
combined mode 10-8
redundant mode 10-8
power management limitations in Catalyst 4500 Switch 10-9
power management mode
selecting 10-8
Power-On-Self-Test diagnostics 48-3, 48-14
Power-On-Self-Test for Supervisor Engine V-10GE 48-8
power redundancy-mode command 10-11
power supplies
available power for Catalyst 4500 Switch 10-13
fixed 10-7
variable 10-7, 10-20
primary VLANs 40-2, 40-5
associating with secondary VLANs 40-14
configuring as a PVLAN 40-13
priority
overriding CoS of incoming frames 33-4
priority queuing, QoS on Sup 6-E 32-84
private VLAN
configure port security 35-14
enabling DHCP Snooping 37-11
private VLANs
across multiple switches 40-5
and SVIs 40-10
benefits of 40-2
community ports 40-4
community VLANs 40-3, 40-4
default configuration 40-11
end station access to 40-3
isolated port 40-4
isolated VLANs 40-3, 40-4
ports
community 40-4
isolated 40-4
promiscuous 40-5
primary VLANs 40-2, 40-5
promiscuous ports 40-5
secondary VLANs 40-3
subdomains 40-2
traffic in 40-9
privileged EXEC mode 2-5
privileges
changing default 3-23
configuring levels 3-23
exiting 3-24
logging in 3-24

promiscuous ports
configuring PVLAN 40-15
defined 40-5
setting mode 40-22
protocol timers 17-4
provider edge devices 31-2
pruning, VTP
See VTP pruning
pseudobridges
description 17-25
PVACL 37-16
PVID (port VLAN ID)
and 802.1X with voice VLAN ports 34-18
PVLAN promiscuous trunk port
configuring 40-2, 40-15, 40-19
PVLANs
802.1q support 40-12
across multiple switches 40-5
configuration guidelines 40-11
configure port security 35-13, 35-15, 35-17
configure port security in a wireless setting 35-31
configure port security over Layer 2 EtherChannel 35-31
configuring 40-10
configuring a VLAN 40-13
configuring promiscuous ports 40-15
host ports
configuring a Layer 2 interface 40-16
setting 40-22
overview 40-1
permitting routing, example 40-21
promiscuous mode
setting 40-22
setting
interface mode 40-22

Q

QoS
allocating bandwidth 32-56
and software processed packets 32-16
auto-QoS
configuration and defaults display 32-20
configuration guidelines 32-19
described 32-17
displaying 32-20
effects on NVRAM configuration 32-19
enabling for VoIP 32-19
basic model 32-5
burst size 32-31
classification 32-6 to 32-10
configuration guidelines 32-25
auto-QoS 32-19
configuring
auto-QoS 32-17
DSCP maps 32-57
dynamic buffer limiting 32-27
traffic shaping 32-56
trusted boundary 32-26
configuring Layer 2 Control Packet QoS, feature interaction 32-64
configuring Layer 2 Control Packet QoS, guidelines 32-64
configuring Layer 2 Control Packet QoS, overview 32-60
configuring UBRL 32-42
configuring VLAN-based on Layer 2 interfaces 32-51
creating named aggregate policers 32-31
creating policing rules 32-32
default auto configuration 32-17
default configuration 32-23
definitions 32-3
disabling on interfaces 32-40
enabling and disabling 32-50
enabling hierarchical policers 32-46
enabling on interfaces 32-40
enabling per-port per-VLAN 32-48
flowcharts 32-8, 32-12
IP phones

automatic classification and queueing 32-17
detection and trusted settings 32-17, 32-26
overview 32-1
overview of per-port per-VLAN 32-16
packet modification 32-16
port-based 32-51
priority 32-15
traffic shaping 32-16
transmit rate 32-56
trust states
trusted device 32-26
VLAN-based 32-51
See also COS; DSCP values; transmit queues
QoS active queue management
tracking queue length 32-14
QoS labels
definition 32-3
QoS mapping tables
CoS-to-DSCP 32-57
DSCP-to-CoS 32-59
policed-DSCP 32-58
types 32-14
QoS marking
description 32-5
QoS on Sup 6-E
Active Queue management via DBL 32-85
active queue management via DBL 32-81, 32-85
classification 32-71
configuring 32-67
configuring the policy map marking action 32-77
hardware capabilities for marking 32-77
hierarchical policies 32-87
how to implement policing 32-72
marking action drivers 32-75
marking network traffic 32-72
MQC-based QoS configuration 32-68
multi-attribute marking support 32-76
platform hardware capabilities 32-70
platform restrictions 32-72
platform-supported classification criteria and QoS features 32-68, 32-69
policing 32-71
policy associations 32-89
prerequisites for applying a service policy 32-70
priority queuing 32-84
restrictions for applying a service policy 32-70
shaping 32-79
sharing(bandwidth) 32-81
sharing(blandwidth), shapring, and priority queuing 32-79
software QoS 32-89
traffic marking procedure flowchart 32-75
QoS policers
burst size 32-31
types of 32-10
QoS policing
definition 32-5
described 32-5, 32-10
QoS policy
attaching to interfaces 32-11
overview of configuration 32-33
QoS service policy
prerequisites 32-70
restrictions for applying 32-70
QoS transmit queues
allocating bandwidth 32-56
burst 32-16
configuring traffic shaping 32-56
mapping DHCP values to 32-55
maximum rate 32-16
overview 32-14
sharing link bandwidth 32-15
QoS transmit queues, configuring 32-54
Quality of service
See QoS
queueing 32-6, 32-14

R

RADIUS server
- configure to-Switch communication 34-26
- configuring settings 34-28
- parameters on the switch 34-26

range command 6-4

range macros
- defining 6-5

ranges of interfaces
- configuring 6-4

Rapid Spanning Tree
- See RSTP

rcommand command 12-12

re-authentication of a client
- configuring manual 34-47
- enabling periodic 34-42

reduced MAC address 17-2

redundancy
- configuring 8-7
- guidelines and restrictions 8-6
  - changes made through SNMP 8-11
- NSF-aware support 9-2
- NSF-capable support 9-2
- overview 8-2
- redundancy command 8-8
- understanding synchronization 8-5

redundancy (NSF) 9-1
- configuring
  - BGP 9-11
  - CEF 9-11
  - EIGRP 9-16
  - IS-IS 9-14
  - OSPF 9-13
- routing protocols 9-5

redundancy (RPR)
- route processor redundancy 8-3
- synchronization 8-5

redundancy (SSO)
- redundancy command 9-10
- route processor redundancy 8-3
- synchronization 8-5

related documentation xl

reload command 3-28, 3-29

Remote Network Monitoring
- See RMON

replication
- description 29-8

report suppression, IGMP
- disabling 21-11

reserved-range VLANs
- See VLANs

reset command 51-3

resetting an interface to default configuration 6-26

resetting a switch to defaults 3-31

restricting access
- NTP services 4-8
- TACACS+ 3-15

retransmission number
- setting in 802.1X authentication 34-46

retransmission time
- changing in 802.1X authentication 34-45

RFC
- 1157, SNMPv1 45-2
- 1305, NTP 4-2
- 1757, RMON 47-2
- 1901, SNMPv2C 45-2
- 1902 to 1907, SNMPv2 45-2
- 2273-2275, SNMPv3 45-2

RIP
- description 1-9

RMON
- default configuration 47-3
- displaying status 47-7
- enabling alarms and events 47-4
- groups supported 47-2
- overview 47-1

ROM monitor

boot process and 3-26
CLI 2-7
commands 51-2 to 51-3
debug commands 51-5
entering 51-2
exiting 51-6
overview 51-1
root bridge
configuring 17-9
selecting in MST 17-22
root guard
and MST 17-23
enabling 18-2
overview 18-2
routed packets
ACLs 39-32
route-map (IP) command 30-3
route maps
defining 30-3
PBR 30-2
router ACLs
description 39-3
using with VLAN maps 39-31
router ACLs, using PACL with VLAN maps 39-37
route targets
VPN 31-4
Routing Information Protocol
See RIP
RPF
<Emphasis>See Unicast RPF
RSPAN
configuration guidelines 43-16
destination ports 43-5
IDS 43-2
monitored ports 43-4
monitoring ports 43-5
received traffic 43-3
sessions
creating 43-17
defined 43-3
limiting source traffic to specific VLANs 43-23
monitoring VLANs 43-22
removing source (monitored) ports 43-21
specifying monitored ports 43-17
source ports 43-4
transmitted traffic 43-4
VLAN-based 43-5
RSTP
compatibility 17-23
description 17-22
port roles 17-24
port states 17-24

S

SAID
See 802.10 SAID
scheduling 32-14
defined 32-5
overview 32-6
secondary root switch 17-12
secondary VLANs 40-3
associating with primary 40-14
permitting routing 40-21
security
configuring 36-1
Security Association Identifier
See 802.10 SAID
selecting a power management mode 10-8
selecting X2/TwinGig Convertor Mode 6-8
sequence numbers in log messages 44-7
servers, VTP
See VTP servers
service-policy command 32-33
service-policy input command 25-2, 32-40
service-provider networks
and customer VLANs 22-2
set default interface command 30-4

set interface command 30-3
set ip default next-hop command 30-4
set ip next-hop command 30-3
set-request operation 45-4
severity levels, defining in system messages 44-8
shaping, QoS on Sup 6-E 32-79
sharing(bandwidth), QoS on Sup 6-E 32-81
show adjacency command 27-9
show boot command 3-31
show catalyst4000 chassis-mac-address command 17-3
show cdp command 23-2, 23-3
show cdp entry command 23-4
show cdp interface command 23-3
show cdp neighbors command 23-4
show cdp traffic command 23-4
show ciscoview package command 4-33
show ciscoview version command 4-33
show cluster members command 12-12
show configuration command 6-13
show debugging command 23-4
show environment command 10-2
show history command 2-4
show interfaces command 6-18, 6-23, 6-25
show interfaces status command 7-2
show ip cache flow aggregation destination-prefix command 46-12
show ip cache flow aggregation prefix command 46-12
show ip cache flow aggregation source-prefix command 46-12
show ip cache flow command 46-9
show ip cef command 27-8
show ip eigrp interfaces command 26-18
show ip eigrp neighbors command 26-18
show ip eigrp topology command 26-18
show ip eigrp traffic command 26-18
show ip interface command 29-16
show ip local policy command 30-5
show ip mroute command 29-16
show ip pim interface command 29-16
show l2protocol command 22-12
show mac-address-table address command 7-3
show mac-address-table interface command 7-3
show mls entry command 27-8
show module command 7-1, 17-5
show PoE consumed 11-7
show power inline command 11-6
show power inline consumption command 11-5
show power supplies command 10-11
show protocols command 6-23
show running-config command
  adding description for an interface 6-13
  checking your settings 3-9
  displaying ACLs 39-24, 39-27, 39-34, 39-35
show startup-config command 3-10
show users command 7-6
show version command 3-29
shutdown, command 6-24
shutdown threshold for Layer 2 protocol packets 22-9
shutting down
  interfaces 6-24
Simple Network Management Protocol
  See SNMP
single spanning tree
  See SST
slot numbers, description 6-2
Smartports macros
  applying global parameter values 16-8
  applying macros 16-8
  applying parameter values 16-8
  configuration guidelines 16-5
  configuring 16-2
  creating 16-7
  default configuration 16-3
  defined 16-1
  displaying 16-13
  tracing 16-6
SNMP
  accessing MIB variables with 45-4

agent
described 45-4
disabling 45-7
authentication level 45-10
community strings
configuring 45-7
overview 45-4
configuration examples 45-16
configuration guidelines 45-6
default configuration 45-6
enabling 50-16
engine ID 45-6
groups 45-6, 45-9
host 45-6
informs
and trap keyword 45-11
described 45-5
differences from traps 45-5
enabling 45-14
limiting access by TFTP servers 45-15
limiting system log messages to NMS 44-9
manager functions 45-3
notifications 45-5
overview 45-1, 45-4
status, displaying 45-17
system contact and location 45-15
trap manager, configuring 45-13
traps
described 45-3, 45-5
differences from informs 45-5
enabling 45-11
enabling MAC address notification 4-22
enabling MAC move notification 4-24
enabling MAC threshold notification 4-26
overview 45-1, 45-4
types of 45-11
users 45-6, 45-9
versions supported 45-2
SNMP commands 50-16
SNMPv1 45-2
SNMPv2C 45-2
SNMPv3 45-2
software
upgrading 8-13
software configuration register 3-26
software QoS, on Sup 6-E 32-89
software switching
description 27-5
interfaces 27-6
key data structures used 29-7
SPAN
and ACLs 43-5
configuration guidelines 43-7
configuring 43-6 to 43-10
destination ports 43-5
IDS 43-2
monitored port, defined 43-4
monitoring port, defined 43-5
received traffic 43-3
sessions
defined 43-3
source ports 43-4
transmitted traffic 43-4
VLAN-based 43-5
SPAN and RSPAN
concepts and terminology 43-3
default configuration 43-6
displaying status 43-25
overview 43-1
session limits 43-6
SPAN enhancements
access list filtering 43-13
configuration example 43-16
CPU port sniffing 43-10
encapsulation configuration 43-12
ingress packets 43-12
packet type filtering 43-15
spanning-tree backbonefast command 18-16

spanning-tree cost command 17-15
spanning-tree guard root command 18-2
spanning-tree portfast bpdu-guard command 18-8
spanning-tree portfast command 18-7
spanning-tree port-priority command 17-13
spanning-tree uplinkfast command 18-12
spanning-tree vlan
  command 17-9
  command example 17-9
spanning-tree vlan command 17-8
spanning-tree vlan cost command 17-15
spanning-tree vlan forward-time command 17-19
spanning-tree vlan hello-time command 17-17
spanning-tree vlan max-age command 17-18
spanning-tree vlan port-priority command 17-13
spanning-tree vlan priority command 17-17
spanning-tree vlan root primary command 17-10
spanning-tree vlan root secondary command 17-12
speed
  configuring interface 6-11
speed command 6-11
SSO
  configuring 9-10
SSO operation 9-4
SST
  description 17-22
  interoperability 17-24
static addresses
  See addresses
static routes
  configuring 3-11
  verifying 3-12
statistics
  displaying 802.1X 34-48
  displaying PIM 29-20
  NetFlow accounting 46-9
  SNMP input and output 45-17
sticky learning
  configuration file 35-5
  defined 35-5
  disabling 35-5
  enabling 35-5
  saving addresses 35-5
sticky MAC addresses
  configuring 35-7
  defined 35-4
Storm Control
  displaying 42-7
  enabling Broadcast 42-3
  enabling Multicast 42-4
  hardware-based, implementing 42-2
  overview 42-1
  software-based, implementing 42-2
STP
  bridge ID 17-2
  configuring 17-7 to 17-20
  creating topology 17-4
  defaults 17-6
  disabling 17-19
  enabling 17-7
  enabling extended system ID 17-8
  enabling Per-VLAN Rapid Spanning Tree 17-20
  EtherChannel guard
    disabling 18-6
  forward-delay time 17-18
  hello time 17-17
  Layer 2 protocol tunneling 22-7
  maximum aging time 17-18
  overview 17-1, 17-3
  per-VLAN rapid spanning tree 17-6
  port cost 17-15
  port priority 17-13
  root bridge 17-9
stratum, NTP 4-2
stub routing (EIGRP)
  benefits 26-17
  configuration tasks 26-17
  configuring 26-13

overview 26-12, 26-13
restrictions 26-17
verifying 26-18
subdomains, private VLAN 40-2
summer time 4-13
supervisor engine
accessing the redundant 8-15
configuring 3-8 to 3-13
copying files to standby 8-15
default configuration 3-1
default gateways 3-11
environmental monitoring 10-1
redundancy 9-1
ROM monitor 3-26
startup configuration 3-25
static routes 3-11
synchronizing configurations 8-11
Supervisor Engine II-TS
insufficient inline power handling 10-18, 11-11
SVI Autostate Exclude
understanding 26-3
SVI Autostate exclude
configuring 26-7
switched packets
and ACLs 39-31
Switched Port Analyzer
See SPAN
switching, NetFlow
checking for required hardware 46-6
configuration (example) 46-13
configuring switched IP flows 46-8
enabling Collection 46-7
exporting cache entries 46-9
switchport
show interfaces 6-18, 6-25
switchport access vlan command 15-6, 15-8
switchport block multicast command 41-2
switchport block unicast command 41-2
switchport mode access command 15-8
switchport mode dot1q-tunnel command 22-6
switchport mode dynamic command 15-6
switchport mode trunk command 15-6
switch ports
See access ports
switchport trunk allowed vlan command 15-6
switchport trunk encapsulation command 15-6
switchport trunk encapsulation dot1q command 15-3
switchport trunk encapsulation isl command 15-3
switchport trunk encapsulation negotiate command 15-3
switchport trunk native vlan command 15-6
switchport trunk pruning vlan command 15-7
switch-to-RADIUS server communication
configuring 34-26
sysret command 51-5
system
reviewing configuration 3-10
settings at startup 3-27
system alarms
on Sup 2+ to V-10GE 10-5
on Sup 6-E 10-5
overview 10-4
system clock
configuring
daylight saving time 4-13
manually 4-11
summer time 4-13
time zones 4-12
displaying the time and date 4-12
overview 4-2
See also NTP
system images
loading from Flash memory 3-30
modifying boot field 3-27
specifying 3-30
system message logging
default configuration 44-3
defining error message severity levels 44-8
disabling 44-4

displaying the configuration 44-12
enabling 44-4
facility keywords, described 44-11
level keywords, described 44-8
limiting messages 44-9
message format 44-2
overview 44-1
sequence numbers, enabling and disabling 44-7
setting the display destination device 44-4
synchronizing log messages 44-5
timestamps, enabling and disabling 44-7
UNIX syslog servers
configuring the daemon 44-10
configuring the logging facility 44-11
facilities supported 44-11
system MTU
802.1Q tunneling 22-5
maximums 22-5
system name
default configuration 4-15
default setting 4-15
manual configuration 4-15
See also DNS
system prompt, default setting 4-14, 4-15

T

TACACS+ 36-1
accounting, defined 3-16
authentication, defined 3-16
authorization, defined 3-16
configuring
accounting 3-21
authentication key 3-18
authorization 3-21
login authentication 3-19
default configuration 3-18
displaying the configuration 3-22
identifying the server 3-18
limiting the services to the user 3-21
operation of 3-17
overview 3-15
tracking services accessed by user 3-21
tagged packets
802.1Q 22-3
Layer 2 protocol 22-7
TCAM programming algorithm
changing 39-9
TCAM programming algorithm, overview 39-7
TCAM programming and ACLs 39-10, 39-12
for Sup II-Plust thru V-10GE 39-6
TCAM programming and ACLs for Sup 6-E 39-15
TCAM region, changing the algorithm 39-9
TCAM region, resizing 39-10
TDR
checking cable connectivity 7-3
enabling and disabling test 7-3
guidelines 7-3
Telnet
accessing CLI 2-2
disconnecting user sessions 7-6
executing 7-5
monitoring user sessions 7-6
telnet command 7-5
Terminal Access Controller Access Control System Plus
See TACACS+
TFTP
configuration files in base directory 3-4
configuring for autoconfiguration 3-4
limiting access by servers 45-15
TFTP download
See also console download
time
See NTP and system clock
Time Domain Reflectometer
See TDR
time exceeded messages 7-8
timer

See login timer
timestamps in log messages 44-7
time zones 4-12
Token Ring
media not supported (note) 13-5, 13-9
Topology change notification processing
MLD Snooping
Topology change notification processing 21-5
TOS
description 32-4
trace command 7-9
traceroute
See IP traceroute
See Layer 2 Traceroute
traceroute mac command 7-10
traceroute mac ip command 7-10
traffic
blocking flooded 41-2
traffic control
using ACLs (figure) 39-4
using VLAN maps (figure) 39-5
traffic marking procedure flowchart 32-75
traffic shaping 32-16
translational bridge numbers (defaults) 13-4
transmit queues
See QoS transmit queues
transmit rate 32-56
traps
configuring MAC address notification 4-22
configuring MAC move notification 4-24
configuring MAC threshold notification 4-26
configuring managers 45-11
defined 45-3
enabling 4-22, 4-24, 4-26, 45-11
notification types 45-11
overview 45-1, 45-4
troubleshooting
with CiscoWorks 45-4
with system message logging 44-1
with traceroute 7-8
troubleshooting high CPU due to ACLs 39-12
trunk ports
configure port security 35-16
configuring PVLAN 40-17 to 40-19
trunks
802.1Q restrictions 15-5
configuring 15-6
configuring access VLANs 15-6
configuring allowed VLANs 15-6
default interface configuration 15-6
different VTP domains 15-3
enabling to non-DTP device 15-4
encapsulation 15-3
specifying native VLAN 15-6
understanding 15-3
trusted boundary for QoS 32-26
Trust State of interfaces, configuring
trust states
configuring 32-52
tunneling
defined 22-1
tunnel ports
802.1Q, configuring 22-6
described 22-2
incompatibilities with other features 22-5
TwinGig Convertors
limitations on using 6-8
port numbering 6-8
selecting X2/TwinGig Convertor mode 6-8
type of service
See TOS

U

UDLD
default configuration 24-2
disabling 24-3
enabling 24-3

overview 24-1
unauthorized ports with 802.1X 34-4
unicast
See IP unicast
unicast flood blocking
configuring 41-1
unicast MAC address filtering
and adding static addresses 4-29
and broadcast MAC addresses 4-28
and CPU packets 4-29
and multicast addresses 4-28
and router MAC addresses 4-28
configuration guidelines 4-28
described 4-28
unicast MAC address filtering, configuring
ACLs
configuring unicast MAC address filtering 39-19
Unicast RPF (Unicast Reverse Path Forwarding)
applying 28-5
BGP attributes
caution 28-4
CEF
requirement 28-2
tables 28-7
configuring 28-9
(examples) ?? to 28-12
BOOTP 28-8
DHCP 28-8
enterprise network (figure) 28-6
prerequisites 28-9
routing table requirements 28-7
tasks 28-9
verifying 28-10
deploying 28-5
description 28-2
disabling 28-11
enterprise network (figure) 28-6
FIB 28-2
implementing 28-4
maintaining 28-10
monitoring 28-10
packets, dropping (figure) 28-4
prerequisites 28-9
restrictions
basic 28-8
routing asymmetry 28-7
routing asymmetry (figure) 28-8
routing table requirements 28-7
security policy
applying 28-5
attacks, mitigating 28-5
deploying 28-5
tunneling 28-5
source addresses, validating 28-3
(figure) 28-3, 28-4
failure 28-3
traffic filtering 28-5
tunneling 28-5
validation
failure 28-3, 28-4
packets, dropping 28-3
source addresses 28-3
verifying 28-10
unicast traffic
blocking 41-2
unidirectional ethernet
enabling 25-2
example of setting 25-2
overview 25-1
UniDirectional Link Detection Protocol
See UDLD
UNIX syslog servers
daemon configuration 44-10
facilities supported 44-11
message logging configuration 44-11
UplinkFast
and MST 17-23
enabling 18-16

MST and 17-23
overview 18-11
User Based Rate Limiting
configuring 32-42
overview 32-42
user EXEC mode 2-5
user sessions
disconnecting 7-6
monitoring 7-6
using PACL with access-group mode 39-35

V

VACLs
Layer 4 port operations 39-15
virtual configuration register 51-3
virtual LANs
See VLANs
Virtual Private Network
See VPN
VLAN ACLs
See VLAN maps
VLAN-based QoS on Layer 2 interfaces, configuring 32-51
vlan command 13-6
vlan dot1q tag native command 22-4
VLAN ID, discovering 4-30
VLAN Management Policy Server
See VMPS
VLAN maps
applying to a VLAN 39-27
configuration example 39-28
configuration guidelines 39-23
configuring 39-23
creating and deleting entries 39-24
defined 39-3
denying access example 39-29
denying packets 39-24
displaying 39-30
order of entries 39-24
permitting packets 39-24
router ACLs and 39-31
using (figure) 39-5
using in your network 39-27
VLAN maps, PACL and Router ACLs 39-37
VLANs
allowed on trunk 15-6
configuration guidelines 13-3
configuring 13-5
customer numbering in service-provider networks 22-3
default configuration 13-4
description 1-5
extended range 13-3
IDs (default) 13-4
interface assignment 13-7
limiting source traffic with RSPAN 43-23
monitoring with RSPAN 43-22
name (default) 13-4
normal range 13-3
overview 13-1
reserved range 13-3
See also PVLANs
VLAN Trunking Protocol
See VTP
VLAN trunks
overview 15-3
VMPS
configuration file example 13-28
configuring dynamic access ports on client 13-21
configuring retry interval 13-23
database configuration file 13-28
dynamic port membership
example 13-25
reconfirming 13-22
reconfirming assignments 13-22
reconfirming membership interval 13-22
server overview 13-17

VMPS client
administering and monitoring 13-23
configure switch
configure reconfirmation interval 13-22
dynamic ports 13-21
entering IP VMPS address 13-20
reconfirmation interval 13-23
reconfirm VLAM membership 13-22
default configuration 13-20
dynamic VLAN membership overview 13-19
troubleshooting dynamic port VLAN membership 13-24
VMPS server
fall-back VLAN 13-18
illegal VMPS client requests 13-19
overview 13-17
security modes
multiple 13-18
open 13-17
secure 13-18
voice interfaces
configuring 33-1
Voice over IP
configuring 33-1
voice ports
configuring VVID 33-3
voice traffic 11-2, 33-5
voice VLAN
IP phone data traffic, described 33-2
IP phone voice traffic, described 33-2
voice VLAN ports
using 802.1X 34-18
VPN
configuring routing in 31-6
forwarding 31-4
in service provider networks 31-1
routes 31-2
routing and forwarding table
See VRF
VRF
defining 31-4
tables 31-1
VTP
configuration guidelines 13-11
configuring 13-12 to 13-16
configuring transparent mode 13-15
default configuration 13-12
disabling 13-15
Layer 2 protocol tunneling 22-7
monitoring 13-16
overview 13-7
See also VTP version 2
VTP advertisements
description 13-9
VTP clients
configuring 13-14
VTP domains
description 13-8
VTP modes 13-8
VTP pruning
enabling 13-13
overview 13-10
VTP servers
configuring 13-14
VTP statistics
displaying 13-16
VTP version 2
enabling 13-13
overview 13-9
See also VTP
VTY and Network Assistant 12-11
VVID (voice VLAN ID)
and 802.1X authentication 34-18
configuring 33-3

W

Wake-on-LAN

configure with 802.1X 34-39
WCCP
configuration examples 49-9
configuring on a router 49-2, 49-10
features 49-4
restrictions 49-5
service groups 49-6
Web Cache Communication Protocol
See WCCP xxxix, 49-1
web caches
See cache engines
web cache services
description 49-4
web caching
See web cache services
See also WCCP
web scaling 49-1