INDEX

ACLs
applying IPv6 ACLs to a Layer 3 interface 42-16

Numerics

10/100 autonegotiation feature, forced 7-11
10-Gigabit Ethernet or Gigabit Ethernet ports
deploy on WS-X4606-10GE-E and Sup 6-E 7-7
10-Gigabit Ethernet port
deploy with Gigabit Ethernet SFP ports 7-7
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) 12-5
802.1Q
trunks 16-6
802.1Q VLANs
encapsulation 14-3
trunk restrictions 14-5
802.1s
See MST
802.1w
See MST
802.1X
See port-based authentication
802.1X authentication
for Critical Authentication 36-13
for guest VLANs 36-10
for MAC Authentication Bypass 36-11
for Wake-on-LAN 36-14
web-based authentication 36-13
with port security 36-16
with VLAN assignment 36-9
with voice VLAN ports 36-19
802.1X Host Mode 36-6
multiauthentication mode 36-8
multidomain authentication mode 36-7
single-host 36-7
802.3ad
See LACP

A

AAA 39-1
AAA (authentication, authorization, and accounting). See also port-based authentication. 37-1
abbreviating commands 2-5
access control entries
See ACEs
access control entries and lists 39-1
access-group mode, configuring on Layer 2 interface 42-30
access-group mode, using PACL with 42-29
access list filtering, SPAN enhancement 46-13
access ports
configure port security 38-7, 38-22
configuring 14-8
access VLANs 14-6
accounting
with TACACS+ 3-16, 3-21
ACEs
ACLs 42-2
IP 42-2
Layer 4 operation restrictions 42-9
ACEs and ACLs 39-1

ACL assignments, port-based authentication 36-17
ACL assignments and redirect URLs, configure 36-32
ACLs
ACEs 42-2
and SPAN 46-5
and TCAM programming for Sup II-Plus thru V-10GE 42-6
applying on routed packets 42-26
applying on switched packets 42-25
compatibility on the same switch 42-3
configuring with VLAN maps 42-25
CPU impact 42-11
downloadable 37-7
hardware and software support 42-5
IP, matching criteria for port ACLs 42-4
MAC extended 42-12
matching criteria for router ACLs 42-3
port
and voice VLAN 42-4
defined 42-3
limitations 42-5
processing 42-11
selecting mode of capturing control packets 42-7
troubleshooting high CPU 42-6
types supported 42-3
understanding 42-2
VLAN maps 42-5
ACLs and VLAN maps, examples 42-19
acronyms, list of A-1
action drivers, marking 33-19
active queue management 33-9
active queue management via DBL, QoS on Sup 6-E 33-32
active traffic monitoring, IP SLAs 50-1
addresses
displaying the MAC address table 4-30
dynamic
changing the aging time 4-21
defined 4-19
learning 4-20
removing 4-22
IPv6 43-2
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
LLDP 1-4, 23-2
advertisements, VTP
See VTP advertisements
aggregation switch, enabling DHCP snooping 40-9
aging time
MAC address table 4-21
All Auth manager sessions, displaying summary 36-68
All Auth manager sessions on the switch authorized for a specified authentication method 36-68
applying IPv6 ACLs to a Layer 3 interface 42-16
AQM via DBL, QoS on Sup 6-E 33-32
ARP
defined 4-30
table
address resolution 4-30
managing 4-30
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) 39-1
Authentication Failed VLAN assignment

configure with 802.1X 36-53
Authentication methods registered with the Auth manager, determining 36-67
authentication open comand 36-8
authentication proxy web pages 37-4
authentication server
defined 36-3
RADIUS server 36-3
Auth manager session for an interface, verifying 36-68
Auth manager summary, displaying 36-67
authoritative time source, described 4-2
authorization
with TACACS+ 3-16, 3-21
authorized and unauthorized ports 36-4
authorized ports with 802.1X 36-4
autoconfiguration 3-2
Auto-MDIX on a port
configuring 7-22
displaying the configuration 7-22
overview 7-21
autonegotiation feature
forced 10/100Mbps 7-11
auto-sync command 5-8

B

Baby Giants
interacting with 7-20
BackboneFast
adding a switch (figure) 18-4
and MST 16-23
configuring 18-16
link failure (figure) 18-14, 18-15
not supported MST 16-23
understanding 18-14
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 54-3
BGP 1-11
routing session with multi-VRF CE 31-11
blocking packets 44-1
blocking state (STP)
RSTP comparisons (table) 16-24
boot bootldr command 3-31
boot command 3-28
boot commands 54-3
boot fields
See configuration register boot fields
boot system command 3-26, 3-31
boot system flash command 3-28
Border Gateway Protocol
See BGP
boundary ports
description 16-27
BPDU Guard
and MST 16-23
configuring 18-16
overview 18-8
BPDUs
and media speed 16-2
pseudobridges and 16-25
what they contain 16-3
bridge ID
See STP bridge ID
bridge priority (STP) 16-16
bridge protocol data units
See BPDUs
Broadcast Storm Control
disabling 45-5
enabling 45-3

C

Call Home
- description 1-16, 52-1
- message format options 52-2
- messages
  - format options 52-2

call home 52-1
- alert groups 52-6
- configuring e-mail options 52-9
- contact information 52-4
- default settings 52-18
- destination profiles 52-5
- displaying information 52-14
- mail-server priority 52-10
- pattern matching 52-9
- periodic notification 52-8
- rate limit messages 52-9
- severity threshold 52-8
- smart call home feature 52-2
- SMTP server 52-9
- testing communications 52-10

call home alert groups
- configuring 52-6
- description 52-6
- subscribing 52-7

call home contacts
- assigning information 52-4

call home destination profiles
- attributes 52-5
- configuring 52-5
- description 52-5
- displaying 52-16

call home notifications
- full-txt format for syslog 52-25
- XML format for syslog 52-34

Capturing control packets
- selecting mode 42-7

cautions
- Unicast RPF
  - BGP optional attributes 28-5

cautions for passwords
- encrypting 3-22

CDP
- configuration 20-2
- defined with LLDP 23-1
- displaying configuration 20-3
- enabling on interfaces 20-3
- host presence detection 36-8
- maintaining 20-3
- monitoring 20-3
- overview 1-2, 20-1

cdp enable command 20-3

CEF
- adjacency tables 27-2
- and NSF with SSO 9-4
- configuring load balancing 27-7
- displaying statistics 27-8
- enabling 27-6, 53-2
- hardware switching 27-4
- load balancing 27-6
- overview 27-2
- software switching 27-4

certificate authority (CA) 52-3

CGMP
- overview 21-1

channel-group group command 19-8, 19-10

Cisco 7600 series Internet router
- enabling SNMP 55-4, 55-5

Cisco Discovery Protocol
- See CDP

Cisco Express Forwarding
- See CEF

Cisco Group Management Protocol
- See CGMP

Cisco IOS IP SLAs 50-2

Cisco IOS NSF-aware
- support 9-2

Cisco IOS NSF-capable support 9-2
Cisco IP Phones
configuring 34-3
sound quality 34-1
CiscoWorks 2000 49-4
CIST
description 16-22
civic location 23-3
class level, configure in a service policy 33-29
class of service
See CoS
clear cdp counters command 20-4
clear cdp table command 20-3
clear counters command 7-25
clearing
IP multicast table entries 29-26
clear ip eigrp neighbors command 26-17
CLI
accessing 2-2
backing out one level 2-5
getting commands 2-5
history substitution 2-4
modes 2-5
monitoring environments 46-1
ROM monitor 2-7
software basics 2-4
clients
in 802.1X authentication 36-3
clock
See system clock
command-line processing 2-3
command modes 2-5
commands
b 54-3
boot 54-3
dev 54-3
dir device 54-3
i 54-3
listing 2-5
reset 54-3
ROM monitor 54-2 to ??
SNMP 55-4
common and internal spanning tree
See CIST
common spanning tree
See CST
community ports 35-4
community strings
configuring 49-7
overview 49-4
community VLANs 35-3, 35-4
and SPAN features 35-12
configure as a PVLAN 35-13
compiling MIBs 55-4
config-register command 3-29
config terminal command 3-9
configurable leave timer,IGMP 21-4
configuration examples
SNMP 49-16
configuration files
limiting TFTP server access 49-15
obtaining with DHCP 3-6
saving 3-10
system contact and location information 49-15
configuration guidelines
SNMP 49-6
configuration register
boot fields
listing value 3-29
modifying 3-28
changing from ROM monitor 54-3
changing settings 3-28 to 3-29
configuring 3-26
settings at startup 3-27
configure class-level queue-limit in a service policy 33-29
configure terminal command 3-29, 7-2
configuring access-group mode on Layer 2 interface 42-30

configuring flow control 7-14
configuring interface link and trunk status envents 7-26
configuring named IPv6 ACLs 42-15
configuring named MAC extended ACLs 42-12, 42-14
configuring unicast MAC address filtering 42-12
configuring VLAN maps 42-17
console configuration mode 2-5
console port
  disconnecting user sessions 8-7
  monitoring user sessions 8-6
contact information
  assigning for call home 52-4
control plane policing
  See CoPP
control protocol, IP SLAs 50-4
CoPP
  applying QoS service policy to control plane 39-3
  configuring
    ACLs to match traffic 39-3
    enabling MLS QoS 39-3
    packet classification criteria 39-3
    service-policy map 39-3
  control plane configuration mode
    entering 39-3
  displaying
    dynamic information 39-7
    number of conforming bytes and packets 39-7
    rate information 39-7
  entering control plane configuration mode 39-3
  monitoring statistics 39-7
  overview 39-2
copy running-config startup-config command 3-10
copy system:running-config nvram:startup-config command 3-31
CoS
  definition 33-3
  figure 33-2
  overriding on Cisco IP Phones 34-5
  priority 34-5
counters
  clearing MFIB 29-26
  clearing on interfaces 7-25
CPU, impact of ACL processing 42-11
CPU port sniffing 46-10
crashinfo
  kernel file 3-34
  process core dump file 3-34
  process file 3-33
crashinfo, configuring
  commands 3-35
  default 3-35
  determining the process that crashed 3-39
  enabling generation of process core dump 3-38
  saving files to a secondary device 3-39
  show commands 3-36
Critical Authentication
  configure with 802.1X 36-50
CST
  description 16-25
  IST and 16-22
  MST and 16-22
customer edge devices 31-2

D

database agent
  configuration examples 40-15
  enabling the DHCP Snooping 40-12
daylight saving time 4-13
default configuration
  802.1X 36-23
  banners 4-18
  DNS 4-16
  IGMP filtering 21-20
  IGMP snooping 22-5, 22-6
  IP SLAs 50-7
  IPv6 43-7
  LLDP 23-3

MAC address table 4-21
multi-VRF CE 31-3
NTP 4-4
private VLANs 35-11
resetting the interface 7-28
RMON 51-3
SNMP 49-5
SPAN and RSPAN 46-6
system message logging 47-3
TACACS+ 3-18
default gateway
configuring 3-11
verifying configuration 3-11
default settings, erase commad 3-32
default web-based authentication configuration
802.1X 37-6
denial-of-service attacks
IP address spoofing, mitigating 28-5
Unicast RPF, deploying 28-5
denying access to a server on another VLAN 42-23
deploying 10-Gigabit Ethernet and a Gigabit Ethernet SFP ports 7-7
deploying 10-Gigabit Ethernet and a Gigabit Ethernet SFP ports on WS-X4606-10GE-E and Sup 6-E 7-7
description command 7-14
detecting unidirectional links 24-1
dev command 54-3
device discovery protocol 23-1
device IDs
call home format 52-21, 52-22
DHCP
configuring
rate limit for incoming packets 40-13
denial-of-service attacks, preventing 40-13
rate limiting of packets
configuring 40-13
DHCP-based autoconfiguration
client request message exchange 3-3
configuring
client side 3-3
DNS 3-5
relay device 3-5
server-side 3-4
TFTP server 3-4
example 3-7
lease options
for IP address information 3-4
for receiving the configuration file 3-4
overview 3-2
relationship to BOOTP 3-3
DHCP option 82
overview 40-4
DHCP Snooping
enabling, and Option 82 40-10
DHCP snooping
accepting untrusted packets form edge switch 40-10
configuring 40-6
default configuration 40-7
displaying binding tables 40-18
displaying configuration 40-19
displaying information 40-18
enabling 40-7
enabling on private VLAN 40-11
enabling on the aggregation switch 40-9
enabling the database agent 40-12
message exchange process 40-4
monitoring 40-23
option 82 data insertion 40-4
overview 40-1
Snooping database agent 40-2
DHCP Snooping Database Agent
adding to the database (example) 40-18
enabling (example) 40-15
overview 40-2
reading from a TFTP file (example) 40-16
Diagnostics
online 53-1
troubleshooting 53-7

Power-On-Self-Test
causes of failure 53-20
how it works 53-9
overview 53-9
Power-On-Self-Test for Supervisor Engine V-10GE 53-14
Differentiated Services Code Point values
See DSCP values
DiffServ architecture, QoS 33-2
Digital optical monitoring transceiver support 7-10
Digital Signing 54-6
dir device command 54-3
disabled state
RSTP comparisons (table) 16-24
disabling
broadcast storm control 45-5
disabling multicast storm control 45-6
disconnect command 8-7
displaying
Auth Manager sumary for an interface 36-67
MAB details 36-70
summary of all Auth manager sessions 36-68
summary of all Auth manager sessions on the switch authorized for a specified authentication method 36-68
displaying EtherChannel to a Virtual Switch System 19-14
displaying storm control 45-6
display PoE consumed by a module 11-7
DNS
and DHCP-based autoconfiguration 3-5
default configuration 4-16
displaying the configuration 4-17
overview 4-15
setting up 4-16
domain names
DNS 4-15
Domain Name System
See DNS
downloading MIBs 55-2, 55-3, 55-4
DSCP values
definition 33-4
IP precedence 33-2
DTP
VLAN trunks and 14-3
duplex command 7-13
duplex mode
configuring interface 7-11
dynamic ARP inspection
ARP cache poisoning 41-2
configuring
ACLs for non-DHCP environments 41-11
in DHCP environments 41-5
log buffer 41-14
rate limit for incoming ARP packets 41-16
denial-of-service attacks, preventing 41-16
interface trust state, security coverage 41-3
log buffer
configuring 41-14
logging of dropped packets 41-4
overview 41-1
port channels, their behavior 41-5
priority of static bindings 41-4
purpose of 41-2
rate limiting of ARP packets 41-4
configuring 41-16
validation checks, performing 41-19
Dynamic Host Configuration Protocol snooping
See DHCP snooping
dynamic port VLAN membership
example 12-29
limit on hosts 12-29
reconfirming 12-26
troubleshooting 12-29
Dynamic Trunking Protocol
See DTP

E

EAP frames
- changing retransmission time 36-63
- exchanging (figure) 36-4, 36-6, 36-12
- request/identity 36-3
- response/identity 36-3
- setting retransmission number 36-64

EAPOL frames
- 802.1X authentication and 36-3
- OTP authentication, example (figure) 36-4, 36-12
- start 36-4

edge ports
- description 16-27

EGP
- overview 1-11

EIGRP
- configuration examples 26-18
- monitoring and maintaining 26-17

EIGRP (Enhanced IGRP)
- stub routing
  - benefits 26-16
  - configuration tasks 26-16
  - configuring 26-12
  - overview 26-12
  - restrictions 26-16
  - verifying 26-17

EIGRP (enhanced IGRP)
- overview 1-12

eigrp stub command 26-17

EIGRP stub routing, configuring 26-11

ELIN location 23-3

e-mail addresses
- assigning for call home 52-4

e-mail notifications
- Call Home 1-16, 52-1

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 SNMP 55-4, 55-5

encapsulation types 14-3

Enhanced Interior Gateway Routing Protocol
- See EIGRP

Enhanced PoE support on E-series 11-15

environmental monitoring
- using CLI commands 10-1

EPM logging 36-70

EtherChannel
- channel-group group command 19-8, 19-10
- configuration guidelines 19-5
- configuring 19-6 to 19-14
- configuring Layer 2 19-9
- configuring Layer 3 19-6
- displaying to a virtual switch system 19-14
- 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 19-13

EtherChannel guard
- disabling 18-7
- enabling 18-6
- overview 18-6

explicit host tracking
- enabling 21-11

extended range VLANs
- See VLANs

Extensible Authentication Protocol over LAN 36-2
Exterior Gateway Protocol
See EGP

F

Fallback Authentication
configure with 802.1X 36-57
FastDrop
overview 29-10
FIB
description 27-2
See also MFIB
Filter-ID ACL and Per-User ACL, configureport-based authentication
configure Per-User ACL and Filter-ID ACL 36-38
filtering
in a VLAN 42-17
non-IP traffic 42-12, 42-14
flags 29-11
Flash memory
configuring router to boot from 3-31
loading system images from 3-30
security precautions 3-31
Flexible NetFlow
caveats 32-1
defined 1-2, 32-1
flooded traffic, blocking 44-2
flowchart, traffic marking procedure 33-19
flow control, configuring 7-14
For 11-13
forward-delay time (STP)
configuring 16-18
forwarding information base
See FIB

G

gateway
See default gateway
get-bulk-request operation 49-3
get-next-request operation 49-3, 49-4
get-request operation 49-3, 49-4
get-response operation 49-3
Gigabit Ethernet SFP ports
deploy with 10-Gigabit Ethernet 7-7
global configuration mode 2-5
Guest-VLANs
configure with 802.1X 36-46, 36-54

H

hardware and software ACL support 42-5
hardware switching 27-5
hello time (STP)
configuring 16-17
high CPU due to ACLs, troubleshooting 42-6
history
CLI 2-4
history table, level and number of syslog messages 47-9
hop counts
configuring MST bridges 16-28
host
limit on dynamic port 12-29
host ports
kinds of 35-4
host presence CDP message 36-8
Hot Standby Routing Protocol
See HSRP
HSRP
description 1-10
http
//www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html 50-1, 50-4

//www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/12_4t/fnf_12_4t_book.html 32-1

//www.cisco.com/en/US/docs/ios/fundamentals/command reference/cf_book.html 47-1, 49-1, 51-1

hw-module module num power command 10-18

I

ICMP
enabling 8-12
ping 8-7
running IP traceroute 8-9
time exceeded messages 8-9
ICMP Echo operation
configuring 50-12
IP SLAs 50-11
i command 54-3
IDS
using with SPAN and RSPAN 46-3
IEEE 802.1s
See MST
IEEE 802.1w
See MST
IEEE 802.3ad
See LACP
IGMP
configurable-leave timer 21-4
description 29-3
enabling 29-13
explicit host tracking 21-4
immediate-leave processing 21-3
leave processing, enabling 22-8
overview 21-1
report suppression
disabling 22-10
IGMP filtering
configuring 21-21
default configuration 21-20
described 21-20
monitoring 21-24
IGMP groups
setting the maximum number 21-23
IGMP Immediate Leave
configuration guidelines 21-9
IGMP profile
applying 21-22
configuration mode 21-21
configuring 21-21
IGMP Snooping
configure
leave timer 21-9
configuring
Learning Methods 21-7
static connection to a multicast router 21-8
configuring host statically 21-11
enabling
Immediate-Leave processing
explicit host tracking 21-11
suppressing multicast flooding 21-12
IGMP snooping
configuration guidelines 21-5
default configuration 22-5, 22-6
enabling
globally 21-6
on a VLAN 21-6
enabling and disabling 22-6
IP multicast and 29-4
monitoring 21-14, 22-11
overview 21-1
IGMP Snooping, displaying
group 21-16
hot membership 21-15
how to 21-15
MAC address entries 21-18
multicast router interfaces 21-17
on a VLAN interface 21-18
Querier information 21-19
IGMPSnooping Querier, configuring 21-10

Immediate Leave, IGMP
enabling 22-8
immediate-leave processing
enabling 21-8
IGMP
See fast-leave processing
ingress packets, SPAN enhancement 46-12
inline power
configuring on Cisco IP phones 34-5
Intelligent Power Management 11-4
interacting with Baby Giants 7-20
interface command 3-9, 7-2
interface link and trunk status events
configuring 7-26
interface port-channel command 19-7
interface range command 7-5
interface range macro command 7-6
interfaces
adding descriptive name 7-13
clearing counters 7-25
configuring 7-2
configuring ranges 7-4
displaying information about 7-24
Layer 2 modes 14-4
maintaining 7-24
monitoring 7-24
naming 7-13
numbers 7-2
overview 7-2
restarting 7-25
See also Layer 2 interfaces
Internet Control Message Protocol
See ICMP
Internet Group Management Protocol
See IGMP
Internet Protocol version 6
See IPv6
Inter-Switch Link encapsulation
See ISL encapsulation
Intrusion Detection System
See IDS
inventory management TLV 23-2, 23-7
IP
configuring default gateway 3-11
configuring static routes 3-11
displaying statistics 27-8
IP addresses
128-bit 43-2
discovering 4-30
IPv6 43-2
ip cef command 27-6, 53-2
IP Enhanced IGRP
interfaces, displaying 26-17
ip icmp rate-limit unreachable command 8-12
ip igmp profile command 21-21
ip igmp snooping tcn flood command 21-13
ip igmp snooping tcn flood query count command 21-14
ip igmp snooping tcn query solicit command 21-14
IP information
assigned
through DHCP-based autoconfiguration 3-2
ip load-sharing per-destination command 27-7
ip local policy route-map command 30-8
ip mask-reply command 8-13
IP MTU sizes, configuring 26-8
IP MTU sizes,configuring 26-8
IP multicast
clearing table entries 29-26
configuring 29-12
default configuration 29-12
displaying PIM information 29-21
displaying the routing table information 29-22
enabling dense-mode PIM 29-14
enabling sparse-mode 29-14
features not supported 29-12
hardware forwarding 29-8
IGMP snooping and 21-5, 29-4
overview 29-1

routing protocols 29-2
software forwarding 29-8
See also Auto-RP; IGMP; PIM; RP; RPF
IP multicast routing
enabling 29-13
monitoring and maintaining 29-21
ip multicast-routing command 29-13
IP phones
configuring voice ports 34-3
See Cisco IP Phones 34-1
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 30-7
ip redirects command 8-13
IP routing tables
deleting entries 29-26
IP Service Level Agreements
See IP SLAs
IP service levels, analyzing 50-1
IP SLAs
benefits 50-3
Control Protocol 50-4
default configuration 50-7
definition 50-1
ICMP echo operation 50-11
measuring network performance 50-3
monitoring 50-13
multioperations scheduling 50-6
operation 50-4
responder
described 50-4
enabling 50-8
response time 50-5
scheduling 50-6
SNMP support 50-3
supported metrics 50-3
threshold monitoring 50-6
UDP jitter operation 50-9
IP Source Guard
configuring 40-20
configuring on private VLANs 40-22
displaying 40-22, 40-23
overview 40-19
IP statistics
displaying 27-8
IP traceroute
executing 8-9
overview 8-9
IP unicast
displaying statistics 27-8
IP Unnumbered support
configuring on a range of Ethernet VLANs 13-6
configuring on LAN and VLAN interfaces 13-5
configuring with connected host polling 13-7
DHCP Option 82 13-3
displaying settings 13-8
format of agent remote ID suboptions 13-3
troubleshooting 13-9
with conected host polling 13-4
with DHCP server and Relay agent 13-2
ip unreachables command 8-12
IPv6
addresses 43-2
default configuration 43-7
defined 43-1
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 43-6
Router ID 43-6
OSPF 43-5
IPX
redistribution of route information with EIGRP 1-12
ISL
encapsulation 14-3
isolated port 35-4
isolated VLANs 35-3, 35-4
ISSU
compatibility matrix 6-13

compatiblity verification using Cisco Feature Navigator 6-14
NSF overview 6-3
perform the process
aborting a software upgrade 6-31
configuring the rollback timer as a safeguard 6-32
displaying a compatibility matrix 6-34
loading the new software on the new standby 6-24
stopping the rollback timer 6-23
switching to the standby 6-21
verify the ISSU state 6-17
verify the redundancy mode 6-16
verify the software installation 6-15
vload the new software on standby 6-18
prerequisites 6-2
process overview 6-6
restrictions 6-2
SNMP support 6-14
SSO overview 6-3
IST
and MST regions 16-22
description 16-22
master 16-27

J

jumbo frames
and ethernet ports 7-18
configuring MTU sizes for 7-19
ports and linecards that support 7-16
understanding MTUs 7-17
understanding support 7-17
VLAN interfaces 7-18

K

keyboard shortcuts 2-3

L

labels, definition 33-3
LACP
system ID 19-4
Layer 2 access ports 14-8
Layer 2 frames
classification with CoS 33-2
Layer 2 interface, configuring access-mode mode on 42-30
Layer 2 interfaces
assigning VLANs 12-7
configuring 14-5
configuring as PVLAN host ports 35-17
configuring as PVLAN promiscuous ports 35-16
configuring as PVLAN trunk ports 35-18
defaults 14-5
disabling configuration 14-9
modes 14-4
show interfaces command 14-7
Layer 2 interface type
resetting 35-22
setting 35-22
Layer 2 switching
overview 14-1
Layer 2 Traceroute
and ARP 8-11
and CDP 8-10
host-to-host paths 8-10
IP addresses and subnets 8-11
MAC addresses and VLANs 8-10
multicast traffic 8-10
multiple devices on a port 8-11
unicast traffic 1-24, 8-10
usage guidelines 8-10
Layer 2 trunks
configuring 14-6
overview 14-3
Layer 3 interface, applying IPv6 ACLs 42-16

Layer 3 interface counters,configuring 26-9
Layer 3 interface counters,understanding 26-3
Layer 3 interfaces
  changing from Layer 2 mode 31-7
  configuration guidelines 26-4
  overview 26-1
    logical 26-2
    physical 26-2
  VLANs as interfaces 26-6
Layer 3 packets
  classification methods 33-2
Layer 4 port operations
  configuration guidelines 42-10
  restrictions 42-9
Leave timer, enabling 21-9
link and trunk status events
  configuring interface 7-26
Link Layer Discovery Protocol
  See CDP
listening state (STP)
  RSTP comparisons (table) 16-24
LLDP
  configuring 23-3
    characteristics 23-4
    default configuration 23-3
  disabling and enabling
    globally 23-5
    on an interface 23-6
  monitoring and maintaining 23-10
  overview 23-1
  transmission timer and holdtime, setting 23-4
LLDP-MED
  configuring
    procedures 23-3
    TLVs 23-7, 23-8
  monitoring and maintaining 23-10
  overview 23-1
  supported TLVs 23-2
load balancing
  configuring for CEF 27-7
  configuring for EtherChannel 19-12
  overview 19-5, 27-6
  per-destination 27-7
location service
  configuring 23-9
location TLV 23-3, 23-7
logging, EPM 36-70
Logical Layer 3 interfaces
  configuring 26-5
login authentication
  with TACACS+ 3-19
login banners 4-17
login timer
  changing 8-6
logoutwarning command 8-6
loop guard
  and MST 16-23
  configuring 18-5
  overview 18-3

M

MAC/PHY configuration status TLV 23-2
MAC addresses
  aging time 4-21
  allocating 16-5
  and VLAN association 4-20
  building tables 4-20, 14-2
  convert dynamic to sticky secure 38-5
  default configuration 4-21
  discovering 4-30
  displaying 4-30, 8-3
  displaying in DHCP snooping binding table 40-19
  dynamic
    learning 4-20
    removing 4-22
  in ACLs 42-12
  static

adding 4-28
allowing 4-29
characteristics of 4-27
dropping 4-29
removing 4-28
sticky 38-4
sticky secure, adding 38-5
MAC Authentication Bypass
configure with 802.1X 36-48
MAC details, displaying 36-70
MAC extended access lists 42-12
macros
See Smartports macros
main-cpu command 5-8
management address TLV 23-2
management options
SNMP 49-1
marking
hardware capabilities 33-21
marking action drivers 33-19
marking network traffic 33-16
marking support, multi-attribute 33-20
match ip address command 30-6
maximum aging time (STP)
configuring 16-18
MDA
configuration guidelines 36-20 to 36-21
described 36-20
messages, to users through banners 4-17
MFIB
CEF 29-5
overview 29-11
MFIB, IP
displaying 29-24
MIBs
compiling 55-4
downloading 55-2, 55-3, 55-4
overview 49-1
SNMP interaction with 49-4
MLD Done messages and Immediate-leave 22-4
MLD messages 22-2
MLD queries 22-3
MLD reports 22-4
MLD Snooping
MLD Done messages and Immediate-leave 22-4
MLD messages 22-2
MLD queries 22-3
MLD reports 22-4
Multicast client aging robustness 22-3
Multicast router discovery 22-3
overview 22-1
Mode of capturing control packets, selecting 42-7
modules
checking status 8-2
monitoring
ACL information 42-34
IGMP
snooping 22-11
IGMP filters 21-24
IGMP snooping 21-14
IP SLAs operations 50-13
multicast router interfaces 22-11
multi-VRF CE 31-17
traffic flowing among switches 51-1
VLAN filters 42-24
VLAN maps 42-24
M-record 16-22
MST
and multiple spanning trees 1-5, 16-22
boundary ports 16-27
BPDUs 16-22
configuration parameters 16-26
configuring 16-29
displaying configurations 16-33
edge ports 16-27
enabling 16-29
hop count 16-28
instances

configuring parameters 16-32
description 16-22
number supported 16-26
interoperability with PVST+ 16-23
link type 16-28
master 16-27
message age 16-28
regions 16-26
restrictions 16-29
to-SST interoperability 16-24
MSTP
EtherChannel guard
enabling 18-6
M-record 16-22
M-tree 16-22
M-tree 16-22
MTUS
understanding 7-17
MTU size
configuring 7-19, 7-20, 7-26, 7-27
default 12-5
multiauthentication mode 36-8
multicast
See IP multicast
Multicast client aging robustness 22-3
multicast groups
static joins 22-7
multicast packets
blocking 44-2
Multicast router discovery 22-3
multicast router interfaces, displaying 21-17
multicast router interfaces, monitoring 22-11
multicast router ports, adding 22-7
multicast routers
flood suppression 21-12
multicast router table
displaying 29-22
Multicast Storm Control
enabling 45-4
disabling 45-6
multidomain authentication
See MDA
multidomain authentication mode 36-7
multioperations scheduling, IP SLAs 50-6
Multiple Authentication
described 36-20
Multiple AuthorizationAuthentication
configuring 36-29
Multiple Domain Authentication 36-29
multiple forwarding paths 1-5, 16-22
multiple-hosts mode 36-7
Multiple Spanning Tree
See MST
multiple VPN routing/forwarding
See multi-VRF CE
multi-VRF CE
components 31-3
configuration example 31-12
default configuration 31-3
defined 31-1
displaying 31-17
monitoring 31-17
network components 31-3
packet-forwarding process 31-3

N

named IPv6 ACLs, configuring
ACLs
configuring named IPv6 ACLs 42-15
named MAC extended ACLs
ACLs
configuring named MAC extended 42-12, 42-14
native VLAN
specifying 14-6
network fault tolerance 1-5, 16-22
network management

configuring 20-1
RMON 51-1
SNMP 49-1
network performance, measuring with IP SLAs 50-3
network policy TLV 23-2, 23-7
Network Time Protocol
See NTP
network traffic, marking 33-16
New Software Features in Release 7.7
TDR 8-3
Next Hop Resolution Protocol
See NHRP
NHRP
support 1-12
non-IP traffic filtering 42-12, 42-14
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 9-7
operation 9-4
NSF-aware
support 9-2
NSF-capable
supervisor engines 9-2
support 9-2
NSF with SSO supervisor engine redundancy
and CEF 9-4
overview 9-3
SSO operation 9-3
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 7-23
Online Diagnostics 53-1
online insertion and removal
See OIR
Open Shortest Path First
See OSPF
operating system images
See system images
Option 82
enabling DHCP Snooping 40-10
OSPF
area concept 1-13
description 1-13
for IPv6 43-5

P

packets
- modifying 33-9

packet type filtering
- overview 46-14
- SPAN enhancement 46-14

PACL, using with access-group mode 42-29

PACL with VLAN maps and router ACLs 42-31

PAgP
- understanding 19-3

passwords
- configuring enable password 3-14
- configuring enable secret password 3-14
- encrypting 3-22
- recovering lost enable password 3-25
- setting line password 3-14

PBR (policy-based routing)
- configuration (example) 30-8
- enabling 30-6
- features 30-2
- overview 30-1
- route-map processing logic 30-3
- route-map processing logic example 30-4
- route maps 30-2
- when to use 30-5

per-port and VLAN Access Control List 40-19

per-port per-VLAN QoS
- enabling 33-33
- overview 33-10

Per-User ACL and Filter-ID ACL, configure 36-38

Per-VLAN Rapid Spanning Tree 16-6
- enabling 16-20
- overview 16-6

PE to CE routing, configuring 31-11

Physical Layer 3 interfaces, configuring 26-10

PIM
- configuring dense mode 29-14
- configuring sparse mode 29-14
- displaying information 29-21
- displaying statistics 29-25
- enabling sparse-dense mode 29-14, 29-15
- overview 29-3

PIM-DM 29-3

PIM on an interface, enabling 29-13

PIM-SM 29-4

PIM-SSM mapping, enabling 29-16

ping
- executing 8-8
- overview 8-7

ping command 8-8, 29-21

PoE 11-7
- configuring power consumption for single device 11-5
- Enhanced PoE support on E-series 11-15
- policing and monitoring 11-11
- power consumption for powered devices
  - Intelligent Power Management 11-4
- power management modes 11-3
- show interface status 11-6

PoE policing
- configuring errdisable recovery 11-14
- configuring on an interface 11-12
- displaying on an interface 11-13
- power modes 11-12

point-to-point
- in 802.1X authentication (figure) 36-2

policing
- how to implement 33-15
- See QoS policing

policing, PoE 11-11

policy associations, QoS on Sup 6-E 33-37

policy-map command 33-14

policy map marking action, configuring 33-21

port ACLs
- and voice VLAN 42-4
- defined 42-3
- limitations 42-5

Port Aggregation Protocol
see PAgP
port-based authentication
802.1X with voice VLAN 36-19
authentication server
defined 37-2
changing the quiet period 36-63
client, defined 36-3, 37-2
configuration guidelines 36-24, 37-6
configure ACL assignments and redirect URLs 36-32
configure switch-to-RADIUS server communication 36-27
configure with Authentication Failed VLAN assignment 36-53
configure with Critical Authentication 36-50
configure with Guest-VLANs 36-46, 36-54
configure with MAC Authentication Bypass 36-48
configure with Wake-on-LAN 36-52
configuring
Multiple Domain Authentication and Multiple Authorization 36-29
RADIUS server 37-10
RADIUS server parameters on the switch 37-8
configuring Fallback Authentication 36-57
configuring Guest-VLAN 36-27
configuring manual re-authentication of a client 36-66
controlling authorization state 36-5
default configuration 36-23, 37-6
described 36-1
device roles 36-2, 37-2
displaying statistics 36-67, 37-13
enabling 36-24
802.1X authentication 37-8
enabling multiple hosts 36-62
enabling periodic re-authentication 36-61
encapsulation 36-3
host mode 36-6
how 802.1X fails on a port 36-21
initiation and message exchange 36-3
method lists 36-24
modes 36-6
multidomain authentication 36-20
multiple-hosts mode, described 36-7
port security
multiple-hosts mode 36-7
ports not supported 36-4
pre-authentication open access 36-8
resetting to default values 36-66
setting retransmission number 36-64
setting retransmission time 36-63
switch
as proxy 37-2
topologies, supported 36-21
using with ACL assignments and redirect URLs 36-17
using with port security 36-16
with Critical Authentication 36-13
with Guest VLANs 36-10
with MAC Authentication Bypass 36-11
with VLAN assignment 36-9
port-channel interfaces
See also EtherChannel
creating 19-7
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 16-15
port description TLV 23-2
PortFast
and MST 16-23
BPDU filter, configuring 18-10
configuring or enabling 18-16
overview 18-7
PortFast BPDU filtering
and MST 16-23

enabling 18-10
overview 18-9
port numbering with TwinGig Convertors 7-7
port priority
configuring MST instances 16-32
configuring STP 16-13
ports
blocking 44-1
checking status 8-2
dynamic VLAN membership
example 12-29
reconfirming 12-26
forwarding, resuming 44-3
See also interfaces
port security
aging 38-5
configuring 38-7
displaying 38-28
guidelines and restrictions 38-33
on access ports 38-7, 38-22
on private VLAN 38-14
host 38-14
promiscuous 38-16
topology 38-15, 38-18, 38-32
on trunk port 38-17
guidelines and restrictions 38-15, 38-18, 38-21, 38-32
port mode changes 38-22
on voice ports 38-22
sticky learning 38-5
using with 802.1X 36-16
violations 38-6
with 802.1X Authentication 38-32
with DHCP and IP Source Guard 38-31
with other features 38-33
port states
description 16-5
port VLAN ID TLV 23-2
power
inline 34-5
power dc input command 10-17
power handling for Supervisor Engine II-TS 11-11
power inline command 11-3
power inline consumption command 11-5
power management
Catalyst 4500 series 10-5
Catalyst 4500 Switch power supplies 10-12
configuring combined mode 10-11
configuring redundant mode 10-10
overview 10-1
redundancy 10-5
power management for Catalyst 4500 Switch
combined mode 10-7
redundant mode 10-7
power management limitations in Catalyst 4500 Switch 10-8
power management mode
selecting 10-7
power management TLV 23-2, 23-7
power negotiation
through LLDP 23-8
Power-On-Self-Test diagnostics 53-9, 53-20
Power-On-Self-Test for Supervisor Engine V-10GE 53-14
power redundancy-mode command 10-10
power supplies
available power for Catalyst 4500 Switch 10-12
fixed 10-6
variable 10-6
pre-authentication open access 36-8
pre-authentication open access. See port-based authentication.
primary VLANs 35-3, 35-5
associating with secondary VLANs 35-14
configuring as a PVLAN 35-13
priority
overriding CoS of incoming frames 34-5
priority queuing, QoS on Sup 6-E 33-28
private VLAN
configure port security 38-14, 38-15

enabling DHCP Snooping 40-11
private VLANs
across multiple switches 35-5
and SVIs 35-10
benefits of 35-3
community ports 35-4
community VLANs 35-3, 35-4
default configuration 35-11
end station access to 35-3
isolated port 35-4
isolated VLANs 35-3, 35-4
ports
community 35-4
isolated 35-4
promiscuous 35-5
primary VLANs 35-3, 35-5
promiscuous ports 35-5
secondary VLANs 35-3
subdomains 35-3
traffic in 35-9
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 35-16
defined 35-5
setting mode 35-22
protocol timers 16-4
provider edge devices 31-2
pruning, VTP
See VTP pruning
pseudobridges
description 16-25
PVACL 40-19
PVID (port VLAN ID)
and 802.1X with voice VLAN ports 36-19
PVLAN promiscuous trunk port
configuring 35-2, 35-16, 35-19
PVLANs
802.1q support 35-13
across multiple switches 35-5
configuration guidelines 35-11
configure port security 38-14, 38-16, 38-18
configure port security in a wireless setting 38-32
configuring 35-10
configuring a VLAN 35-13
configuring promiscuous ports 35-16
host ports
configuring a Layer 2 interface 35-17
setting 35-22
overview 35-1
permitting routing, example 35-21
promiscuous mode
setting 35-22
setting
interface mode 35-22

Q

QoS
classification 33-6 to ??
definitions 33-3
enabling per-port per-VLAN 33-33
overview 33-1
overview of per-port per-VLAN 33-10
packet modification 33-9
traffic shaping 33-9
See also COS; DSCP values; transmit queues
QoS active queue management
tracking queue length 33-9
QoS labels
definition 33-3
QoS marking
description 33-5
QoS on Sup 6-E

Active Queue management via DBL 33-32
active queue management via DBL 33-25, 33-32
classification 33-13
configuring 33-11
configuring the policy map marking action 33-21
hardware capabilities for marking 33-21
how to implement policing 33-15
marking action drivers 33-19
marking network traffic 33-16
MQC-based QoS configuration 33-11
multi-attribute marking support 33-20
platform hardware capabilities 33-12
platform restrictions 33-16
platform-supported classification criteria and QoS features 33-11
policing 33-14
policy associations 33-37
prerequisites for applying a service policy 33-13
priority queuing 33-28
queue-limiting 33-29
restrictions for applying a service policy 33-13
shaping 33-23
sharing(bandwidth) 33-25
sharing(blandwidth), shapring, and priority queuing 33-23
software QoS 33-38
traffic marking procedure flowchart 33-19
QoS policing
definition 33-5
described 33-8
QoS policy
attaching to interfaces 33-8
QoS service policy
prerequisites 33-13
restrictions for applying 33-13
QoS transmit queues
burst 33-9
maximum rate 33-9
sharing link bandwidth 33-9
Quality of service
See QoS
queueing 33-8
queue-limiting, QoS on Sup 6-E 33-29

R

RADIUS server
configure to-Switch communication 36-27
configuring settings 36-29
parameters on the switch 36-27
range command 7-5
range macros
defining 7-6
ranges of interfaces
configuring 7-4
Rapid Spanning Tree
See RSTP
re-authentication of a client
configuring manual 36-66
enabling periodic 36-61
redirect URLs, port-based authentication 36-17
reduced MAC address 16-2
redundancy
configuring 5-7
guidelines and restrictions 5-6
changes made through SNMP 5-11
NSF-aware support 9-2
NSF-capable support 9-2
overview 5-2
redundancy command 5-8
understanding synchronization 5-5
redundancy (NSF) 9-1
configuring
BGP 9-9
CEF 9-8
EIGRP 9-12
OSPF 9-11
routing protocols 9-5

redundancy (RPR)
route processor redundancy 5-3
synchronization 5-5
redundancy (SSO)
redundancy command 9-8
route processor redundancy 5-3
synchronization 5-6
reload command 3-28, 3-29, 3-40
Remote Network Monitoring
See RMON
rendezvous point, configuring 29-16
rendezvous point, configuring single static 29-19
replication
description 29-8
report suppression, IGMP
disabling 22-10
reserved-range VLANs
See VLANs
reset command 54-3
resetting an interface to default configuration 7-28
resetting a switch to defaults 3-32
responder, IP SLAs
described 50-4
enabling 50-8
response time, measuring with IP SLAs 50-5
restricting access
NTP services 4-8
TACACS+ 3-15
retransmission number
setting in 802.1X authentication 36-64
retransmission time
changing in 802.1X authentication 36-63
RFC
1157, SNMPv1 49-2
1305, NTP 4-2
1757, RMON 51-2
1901, SNMPv2C 49-2
1902 to 1907, SNMPv2 49-2
2273-2275, SNMPv3 49-2
RIP
description 1-13
for IPv6 43-5
RMON
default configuration 51-3
displaying status 51-6
enabling alarms and events 51-3
groups supported 51-2
overview 51-1
ROM monitor
boot process and 3-26
CLI 2-7
commands 54-2 to ??
exiting 54-5
root bridge
configuring 16-9
selecting in MST 16-22
root guard
and MST 16-23
enabling 18-2
overview 18-2
routed packets
ACLs 42-26
route-map (IP) command 30-6
route maps
defining 30-6
PBR 30-2
router ACLs
description 42-3
using with VLAN maps 42-25
router ACLs, using PACL with VLAN maps 42-31
route targets
VPN 31-3
Routing Information Protocol
See RIP
RPF
<Emphasis>See Unicast RPF
RSPAN
configuration guidelines 46-16

destination ports 46-5
IDS 46-3
monitored ports 46-4
monitoring ports 46-5
received traffic 46-3
sessions
creating 46-17
defined 46-3
limiting source traffic to specific VLANs 46-23
monitoring VLANs 46-22
removing source (monitored) ports 46-21
specifying monitored ports 46-17
source ports 46-4
transmitted traffic 46-4
VLAN-based 46-5
RSTP
compatibility 16-23
description 16-22
port roles 16-23
port states 16-24

S

SAID
See 802.10 SAID
scheduling 33-8
scheduling, IP SLAs operations 50-6
secondary root switch 16-12
secondary VLANs 35-3
associating with primary 35-14
permitting routing 35-21
security
configuring 39-1
Security Association Identifier
See 802.10 SAID
selecting a power management mode 10-7
selecting X2/TwinGig Convertor Mode 7-8
sequence numbers in log messages 47-7
server IDs
description 52-23
service policy, configure class-level queue-limit 33-29
service-policy input command 25-2
set default interface command 30-7
set interface command 30-7
set ip default next-hop command 30-7
set ip next-hop command 30-6
set-request operation 49-4
severity levels, defining in system messages 47-8
shaping, QoS on Sup 6-E 33-23
sharing(bandwidth), QoS on Sup 6-E 33-25
show adjacency command 27-9
show boot command 3-31
show catalyst4000 chassis-mac-address command 16-3
show cdp command 20-2, 20-3
show cdp entry command 20-3
show cdp interface command 20-3
show cdp neighbors command 20-4
show cdp traffic command 20-4
show ciscoview package command 4-33
show ciscoview version command 4-33
show configuration command 7-13
show debugging command 20-4
show environment command 10-2
show history command 2-4
show interfaces command 7-19, 7-20, 7-24, 7-26, 7-27
show interfaces status command 8-2
show ip cef command 27-8
show ip eigrp interfaces command 26-17
show ip eigrp neighbors command 26-17
show ip eigrp topology command 26-17
show ip eigrp traffic command 26-17
show ip interface command 29-21
show ip local policy command 30-8
show ip mroute command 29-21
show ip pim interface command 29-21
show lldp traffic command 23-10
show mac-address-table address command 8-3
show mac-address-table interface command 8-3

show mls entry command 27-8
show module command 8-2, 16-5
show PoE consumed 11-7
show power inline command 11-6
show power supplies command 10-10
show protocols command 7-24
show running-config command
adding description for an interface 7-13
checking your settings 3-9
displaying ACLs 42-19, 42-21, 42-28, 42-29, 42-30
show startup-config command 3-10
show users command 8-6
show version command 3-29
shutdown, command 7-25
shutting down
interfaces 7-25
Simple Network Management Protocol
See SNMP
single-host mode 36-7
single spanning tree
See SST
single static RP, configuring 29-19
slot numbers, description 7-2
smart call home 52-1
description 52-2
destination profile (note) 52-5
registration requirements 52-3
service contract requirements 52-3
Transport Gateway (TG) aggregation point 52-2
SMARTnet
smart call home registration 52-3
Smartports macros
applying global parameter values 15-8
applying macros 15-8
applying parameter values 15-8
configuration guidelines 15-6
configuring 15-2
creating 15-7
default configuration 15-3
defined 15-1
displaying 15-12
tracing 15-6
SNMP
accessing MIB variables with 49-4
agent
described 49-4
disabling 49-7
and IP SLAs 50-3
authentication level 49-10
community strings
configuring 49-7
overview 49-4
configuration examples 49-16
configuration guidelines 49-6
default configuration 49-5
enabling 55-4, 55-5
engine ID 49-6
groups 49-6, 49-9
host 49-6
informs
and trap keyword 49-11
described 49-5
differences from traps 49-5
enabling 49-15
limiting access by TFTP servers 49-15
limiting system log messages to NMS 47-9
manager functions 49-3
notifications 49-5
overview 49-1, 49-4
status, displaying 49-17
system contact and location 49-15
trap manager, configuring 49-13
traps
described 49-3, 49-5
differences from informs 49-5
enabling 49-11
enabling MAC address notification 4-22
enabling MAC move notification 4-24

enabling MAC threshold notification 4-26
overview 49-1, 49-4
types of 49-11
users 49-6, 49-9
versions supported 49-2
SNMP commands 55-4
SNMPv1 49-2
SNMPv2C 49-2
SNMPv3 49-2
software
upgrading 5-13
software configuration register 3-26
software QoS, on Sup 6-E 33-38
software switching
description 27-5
interfaces 27-6
key data structures used 29-7
source IDs
call home event format 52-22
SPAN
and ACLs 46-5
configuration guidelines 46-7
configuring 46-7 to 46-10
destination ports 46-5
IDS 46-3
monitored port, defined 46-4
monitoring port, defined 46-5
received traffic 46-3
sessions
defined 46-3
source ports 46-4
transmitted traffic 46-4
VLAN-based 46-5
SPAN and RSPAN
concepts and terminology 46-3
default configuration 46-6
displaying status 46-24
overview 46-2
session limits 46-6
SPAN enhancements
access list filtering 46-13
configuration example 46-15
CPU port sniffing 46-10
encapsulation configuration 46-12
ingress packets 46-12
packet type filtering 46-14
spanning-tree backbonefast command 18-16
spanning-tree cost command 16-15
spanning-tree guard root command 18-2
spanning-tree portfast bpdu-guard command 18-9
spanning-tree portfast command 18-7
spanning-tree port-priority command 16-13
spanning-tree uplinkfast command 18-13
spanning-tree vlan
command 16-9
command example 16-9
spanning-tree vlan command 16-8
spanning-tree vlan cost command 16-15
spanning-tree vlan forward-time command 16-19
spanning-tree vlan hello-time command 16-17
spanning-tree vlan max-age command 16-18
spanning-tree vlan port-priority command 16-13
spanning-tree vlan priority command 16-17
spanning-tree vlan root primary command 16-10
spanning-tree vlan root secondary command 16-12
speed
configuring interface 7-11
speed command 7-12
SSO
configuring 9-8
SSO operation 9-3
SST
description 16-22
interoperability 16-24
static addresses
See addresses
static routes
configuring 3-11

verifying 3-12
statistics
802.1X 37-13
displaying 802.1X 36-67
displaying PIM 29-25
LLDP 23-10
LLDP-MED 23-10
SNMP input and output 49-17
sticky learning
configuration file 38-5
defined 38-5
disabling 38-5
enabling 38-5
saving addresses 38-5
sticky MAC addresses
configuring 38-7
defined 38-4
Storm Control
displaying 45-6
enabling Broadcast 45-3
enabling Multicast 45-4
hardware-based, implementing 45-2
overview 45-1
software-based, implementing 45-2
STP
bridge ID 16-2
configuring 16-7 to 16-20
creating topology 16-4
defaults 16-6
disabling 16-19
enabling 16-7
enabling extended system ID 16-8
enabling Per-VLAN Rapid Spanning Tree 16-20
EtherChannel guard
disabling 18-7
forward-delay time 16-18
hello time 16-17
maximum aging time 16-18
overview 16-1, 16-3
per-VLAN rapid spanning tree 16-6
port cost 16-15
port priority 16-13
root bridge 16-9
stratum, NTP 4-2
stub routing (EIGRP)
benefits 26-16
configuration tasks 26-16
configuring 26-12
overview 26-11, 26-12
restrictions 26-16
verifying 26-17
subdomains, private VLAN 35-3
summer time 4-13
supervisor engine
accessing the redundant 5-14
configuring 3-8 to 3-13
copying files to standby 5-14
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 5-11
Supervisor Engine II-TS
insufficient inline power handling 11-11
SVI Autostate Exclude
understanding 26-3
SVI Autostate exclude
configuring 26-6
switch 43-2
switched packets
and ACLs 42-25
Switched Port Analyzer
See SPAN
switchport
show interfaces 7-19, 7-20, 7-26, 7-27

switchport access vlan command 14-6, 14-8
switchport block multicast command 44-2
switchport block unicast command 44-2
switchport mode access command 14-8
switchport mode dynamic command 14-6
switchport mode trunk command 14-6
switch ports
  See access ports
switchport trunk allowed vlan command 14-6
switchport trunk encapsulation command 14-6
switchport trunk encapsulation dot1q command 14-3
switchport trunk encapsulation isl command 14-3
switchport trunk encapsulation negotiate command 14-3
switchport trunk native vlan command 14-6
switchport trunk pruning vlan command 14-7
switch-to-RADIUS server communication
  configuring 36-27
system
  reviewing configuration 3-10
  settings at startup 3-27
system alarms
  on Sup 2+ to V-10GE 10-4
  overview 10-4
system and network statistics, displaying 29-21
system capabilities TLV 23-2
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 description TLV 23-2
system images
  loading from Flash memory 3-30
  modifying boot field 3-27
  specifying 3-30
system message logging
  default configuration 47-3
  defining error message severity levels 47-8
  disabling 47-4
  displaying the configuration 47-12
  enabling 47-4
  facility keywords, described 47-12
  level keywords, described 47-9
  limiting messages 47-9
  message format 47-2
  overview 47-1
  sequence numbers, enabling and disabling 47-7
  setting the display destination device 47-5
  synchronizing log messages 47-6
  timestamps, enabling and disabling 47-7
  UNIX syslog servers
    configuring the daemon 47-10
    configuring the logging facility 47-11
    facilities supported 47-12
system name
  manual configuration 4-15
  See also DNS
system name TLV 23-2
system prompt, default setting 4-14

T

TACACS+ 39-1
  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
TCAM programming and ACLs 42-7
for Sup II-Plust thru V-10GE 42-6
TDR
checking cable connectivity 8-3
enabling and disabling test 8-3
guidelines 8-3
Telnet
accessing CLI 2-2
disconnecting user sessions 8-7
executing 8-5
monitoring user sessions 8-6
telnet command 8-6
Terminal Access Controller Access Control System Plus
See TACACS+
TFTP
configuration files in base directory 3-5
configuring for autoconfiguration 3-4
limiting access by servers 49-15
threshold monitoring, IP SLAs 50-6
time
See NTP and system clock
Time Domain Reflectometer
See TDR
time exceeded messages 8-9
timer
See login timer
timestamps in log messages 47-7
time zones 4-12
TLV
host presence detection 36-8
TLVs
defined 1-4, 23-2
LLDP-MED 23-2
Token Ring
media not supported (note) 12-5, 12-9
Topology change notification processing
MLD Snooping
Topology change notification processing 22-4
TOS
description 33-4
trace command 8-9
traceroute
See IP traceroute
See Layer 2 Traceroute
traceroute mac command 8-11
traceroute mac ip command 8-11
traffic
blocking flooded 44-2
traffic control
using ACLs (figure) 42-4
using VLAN maps (figure) 42-5
traffic marking procedure flowchart 33-19
traffic shaping 33-9
translational bridge numbers (defaults) 12-5
traps
configuring MAC address notification 4-22
configuring MAC move notification 4-24
configuring MAC threshold notification 4-26
configuring managers 49-11
defined 49-3
enabling 4-22, 4-24, 4-26, 49-11
notification types 49-11
overview 49-1, 49-4
troubleshooting
with CiscoWorks 49-4
with system message logging 47-1
with traceroute 8-9
troubleshooting high CPU due to ACLs 42-6
trunk ports
configure port security 38-17
configuring PVLAN 35-18 to 35-19
trunks
802.1Q restrictions 14-5
configuring 14-6

configuring access VLANs 14-6
configuring allowed VLANs 14-6
default interface configuration 14-6
different VTP domains 14-3
enabling to non-DTP device 14-4
encapsulation 14-3
specifying native VLAN 14-6
understanding 14-3
trustpoint 52-3
TwinGig Convertors
port numbering 7-7
selecting X2/TwinGig Convertor mode 7-8
type length value
See TLV
type of service
See TOS

U

UDLD
default configuration 24-2
disabling 24-5
enabling 24-4
overview 24-1
UDP jitter, configuring 50-9
UDP jitter operation, IP SLAs 50-9
unauthorized ports with 802.1X 36-4
unicast
See IP unicast
unicast flood blocking
configuring 44-1
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 42-12
Unicast RPF (Unicast Reverse Path Forwarding)
applying 28-5
BGP attributes
caution 28-5
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 1-15, 28-2
disabling 28-11
enterprise network (figure) 28-6
FIB 28-2
implementing 28-4
maintaining 28-11
monitoring 28-11
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 44-2
unidirectional ethernet
enabling 25-2
example of setting 25-2
overview 25-1
UniDirectional Link Detection Protocol
See UDLD
UNIX syslog servers
daemon configuration 47-10
facilities supported 47-12
message logging configuration 47-11
UplinkFast
and MST 16-23
enabling 18-16
MST and 16-23
overview 18-11
user EXEC mode 2-5
user sessions
disconnecting 8-7
monitoring 8-6
using PACL with access-group mode 42-29

V

VACLs
Layer 4 port operations 42-9
virtual configuration register 54-3
virtual LANs
See VLANs
Virtual Private Network
See VPN
Virtual Switch System(VSS), displaying EtherChannel to 19-14
VLAN ACLs
See VLAN maps
vlan command 12-6
VLAN ID, discovering 4-30
VLAN Management Policy Server
See VMPS
VLAN maps
applying to a VLAN 42-21
configuration example 42-22
configuration guidelines 42-18
configuring 42-17
creating and deleting entries 42-19
defined 42-3
denying access example 42-23
denying packets 42-19
displaying 42-24
order of entries 42-18
permitting packets 42-19
router ACLs and 42-25
using (figure) 42-5
using in your network 42-22
VLAN maps, PACL and Router ACLs 42-31
VLANs
allowed on trunk 14-6
configuration guidelines 12-3
configuring 12-5
default configuration 12-4
description 1-7
extended range 12-3
IDs (default) 12-4
interface assignment 12-7
limiting source traffic with RSPAN 46-23
monitoring with RSPAN 46-22
name (default) 12-4

normal range 12-3
overview 12-1
reserved range 12-3
See also PVLANs
VLAN Trunking Protocol
See VTP
VLAN trunks
overview 14-3
VMPS
configuration file example 12-32
configuring dynamic access ports on client 12-25
configuring retry interval 12-27
database configuration file 12-32
dynamic port membership
example 12-29
reconfirming 12-26
reconfirming assignments 12-26
reconfirming membership interval 12-26
server overview 12-21
VMPS client
administering and monitoring 12-28
configure switch
configure reconfirmation interval 12-26
dynamic ports 12-25
entering IP VMPS address 12-24
reconfirmation interval 12-27
reconfirm VLAM membership 12-26
default configuration 12-24
dynamic VLAN membership overview 12-23
troubleshooting dynamic port VLAN membership 12-29
VMPS server
fall-back VLAN 12-23
illegal VMPS client requests 12-23
overview 12-21
security modes
multiple 12-22
open 12-22
secure 12-22
voice interfaces
configuring 34-1
Voice over IP
configuring 34-1
voice ports
configuring VVID 34-3
voice traffic 11-2, 34-5
voice VLAN
IP phone data traffic, described 34-2
IP phone voice traffic, described 34-2
voice VLAN ports
using 802.1X 36-19
VPN
configuring routing in 31-11
forwarding 31-3
in service provider networks 31-1
routes 31-2
routing and forwarding table
See VRF
VRF
defining 31-3
tables 31-1
VRF-aware services
ARP 31-6, 31-9
configuring 31-6
ftp 31-8
ping 31-7
SNMP 31-7
syslog 31-8
tftp 31-8
traceroute 31-8
uRPF 31-7
VTP
client, configuring 12-16
configuration guidelines 12-12
default configuration 12-13
disabling 12-16
monitoring 12-19
overview 12-7

pruning
configuring 12-15
See also VTP version 2
server, configuring 12-16
statistics 12-19
transparent mode, configuring 12-16
version 2
enabling 12-15
VTP advertisements
description 12-9
VTP domains
description 12-8
VTP modes 12-8
VTP pruning
overview 12-11
VTP versions 2 and 3
overview 12-9
See also VTP
VVID (voice VLAN ID)
and 802.1X authentication 36-19
configuring 34-3

W

Wake-on-LAN
configure with 802.1X 36-52
web-based authentication
authentication proxy web pages 37-4
description 1-25, 36-13, 37-1
web-based authentication, interactions with other features 37-4