INDEX

Numerics

10/100 autonegotiation feature, forced 8-21

10-Gigabit Ethernet or Gigabit Ethernet ports
- deploy on WS-X4606-10GE-E and Sup 6-E 8-13

10-Gigabit Ethernet port
- deploy with Gigabit Ethernet SFP ports 8-12, 8-13

10-slot chassis, support for WS-X46490-CSFP-E 8-17

1400 W DC Power supply
- special considerations 13-21

1400 W DC SP Triple Input power supply
- special considerations 13-22

802.10 SAID (default) 16-5

802.1AE
- standard 44-2

802.1Q
- trunks 21-6
- tunneling
  - compatibility with other features 28-5
  - defaults 28-3
  - described 28-2
- tunnel ports with other features 28-6

802.1Q VLANs
- trunk restrictions 18-4

802.1s
- See MST

802.1w
- See MST

802.1X
- See port-based authentication

802.1X authentication
- Authentication Failed VLAN assignment 45-17
- for Critical Authentication 45-14
- for guest VLANs 45-11
- for MAC Authentication Bypass 45-12
- for Unidirectional Controlled Port 45-15
- VLAN User Distribution 45-16
- web-based authentication 45-14
- with port security 45-19
- with VLAN assignment 45-10
- with voice VLAN ports 45-22

802.1X Host Mode 45-6
- multiauthentication mode 45-8
- multidomain authentication mode 45-7
- single-host 45-7

802.1x-REV 44-2

802.3ad
- See LACP

9000W AC, displaying OBFL 13-4

A

AAA 49-1

AAA (authentication, authorization, and accounting). See also port-based authentication. 47-2

abbreviating commands 2-5

about Wireshark 57-5

access control entries
- See ACEs

access control entries and lists 49-1

access-group mode, configuring on Layer 2 interface 52-31

access-group mode, using PACL with 52-30

access list filtering, SPAN enhancement 56-13

access lists
- using with WCCP 70-8

access ports

and Layer 2 protocol tunneling 28-15
configure port security 48-7, 48-22
configuring 18-7
access VLANs 18-5
accounting
with RADIUS 45-111
with TACACS+ 3-16, 3-21
ACEs
ACLs 52-2
IP 1-40, 52-2
Layer 4 operation restrictions 52-10
ACEs and ACLs 49-1
ACL assignments, port-based authentication 45-20
ACL assignments and redirect URLs, configure 45-38
ACL configuration, displaying a Layer 2 interface 52-32
ACLs
ACEs 52-2
and SPAN 56-5
and TCAM programming for Sup 6-E 52-10
and TCAM programming for Sup II-Plus thru V-10GE 52-6
applying IPv6 ACLs to a Layer 3 interface 52-17
applying on routed packets 52-26
applying on switched packets 52-25
compatibility on the same switch 52-3
configuring with VLAN maps 52-25
CPU impact 52-12
downloadable 47-7
hardware and software support 52-6
IP, matching criteria for port ACLs 52-4
MAC extended 52-14
matching criteria for router ACLs 52-3
port
and voice VLAN 52-4
defined 52-3
processing 52-12
selecting mode of capturing control packets 52-7
troubleshooting high CPU 52-6
types supported 52-3
understanding 52-2
VLAN maps 52-5
ACLs, applying to a Layer 2 interface 52-31
ACLs and VLAN maps, examples 52-19
acronyms, list of A-1
action drivers, marking 41-21, 41-55
activating and deactivating a capture point, Wireshark 57-13
activating and deactivating Wiresharkcapture points, conceptual, Wireshark 57-9
active queue management 41-9
active queue management via DBL, QoS on Sup 6-E 41-34, 41-68
active traffic monitoring, IP SLAs 67-1
adding members to a community 15-9
addresses
displaying the MAC table 4-44
dynamic
changing the aging time 4-30
defined 4-28
learning 4-29
removing 4-31
IPv6 53-2
MAC, discovering 4-44
See MAC addresses
static
adding and removing 4-36
defined 4-28
address resolution 4-44
adjacency tables
description 34-2
displaying statistics 34-9
administrative VLAN
REP, configuring 23-9
administrative VLAN, REP 23-8
advertisements
LLDP 1-7, 30-2
advertisements, VTP
See VTP advertisements
aggregation switch, enabling DHCP snooping 51-9

aging time
MAC address table 4-30
All Auth manager sessions, displaying summary 45-126
All Auth manager sessions on the switch authorized for a specified authentication method 45-126
ANCP client
enabling and configuring 37-2
guidelines and restrictions 37-5
identify a port with DHCP option 82 37-4
identify a port with protocol 37-2
overview 37-1
ANCP protocol
identifying a port with 37-2
applying IPv6 ACLs to a Layer 3 interface 52-17
AQM via DBL, QoS on Sup 6-E 41-34, 41-68
archiving crashfiles information 2-8
ARP
defined 4-44
table
address resolution 4-44
managing 4-44
asymmetrical links, and 802.1Q tunneling 28-3
attachment points, Wireshark 57-6
attributes, RADIUS
vendor-proprietary 45-114
vendor-specific 45-112
authentication
NTP associations 4-4
RADIUS
key 45-104
login 45-106
See also port-based authentication
TACACS+
defined 3-16
key 3-18
login 3-19
Authentication, Authorization, and Accounting (AAA) 49-1
Authentication Failed, configuring 80.1X 45-70
Authentication methods registered with the Auth manager, determining 45-125
authentication open comand 45-8
authentication proxy web pages 47-4
authentication server
defined 45-3
RADIUS server 45-3
Auth manager session for an interface, verifying 45-126
Auth manager summary, displaying 45-126
authoritative time source, described 4-2
authorization
with RADIUS 45-110
with TACACS+ 3-16, 3-21
authorized and unauthorized ports 45-5
authorized ports with 802.1X 45-5
autoconfiguration 3-2
automatic discovery
considerations 15-7
Auto-MDIX on a port
configuring 8-31
displaying the configuration 8-32
overview 8-30
autonegotiation feature
forced 10/100Mbps 8-21
Auto SmartPorts built-in macros
configuring parameters 20-6
Auto SmartPorts macros
built-in macros 20-5
configuration guidelines 20-5
default configuration 20-4
defined 20-1
displaying 20-13
enabling 20-4
IOS shell 20-2, 20-10
Auto Smartports macros
defined 1-2
Auto SmartPorts user-defined macros
configuring 20-10
auto-sync command 10-8, 11-7

Auto SmartPorts macros
See also SmartPorts macros
Auto Smartports macros
See also Smartports macros

B

Baby Giants
interacting with 8-29
BackboneFast
adding a switch (figure) 24-3
and MST 21-23
configuring 24-15
link failure (figure) 24-14, 24-15
not supported MST 21-23
understanding 24-13
See also STP
banners
configuring
login 4-27
message-of-the-day login 4-24
default configuration 4-24
when displayed 4-24
b command 72-3
BFD
and hardware support 38-7
configuration example
BFD in a BGP network 38-25
BFD in an EIGRP network with echo mode enabled by default 38-17
BFD in an OSPF network 38-22
support for static routing 38-27
configuring
Echo mode 38-15
session parameters on the interface 38-8
Slow timer 38-16
support for BGP 38-9
support for dynamic routing protocols 38-9
support for EIGRP 38-10
support for OSPF 38-11
support for static routing 38-13
disabling echo mode without asymmetry 38-16
monitoring and troubleshooting 38-17
neighbor relationships 38-3
operation 38-3
prerequisites 38-2
restrictions 38-2
b flash command 72-3
BGP 1-17
routing session with multi-VRF CE 40-9
blocking packets 54-1
blocking state (STP)
RSTP comparisons (table) 21-24
Boolean expressions in tracked lists 58-4
boot bootldr command 3-31
boot command 3-28
boot commands 72-3
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 21-27
BPDU Guard
and MST 21-23
configuring 24-15
overview 24-8
BPDUs
and media speed 21-2
pseudobridges and 21-25
what they contain 21-3
bridge ID
See STP bridge ID
bridge priority (STP) 21-17

bridge protocol data units
See BPDUs
Broadcast Storm Control
disabling 55-5
enabling 55-3
Built-in macros and user-defined triggers, configuring
mapping 20-9

C

cache engine clusters 70-1
cache engines 70-1
cache farms
See cache engine clusters
Call Home
description 1-24, 66-2
message format options 66-2
messages
format options 66-2
call home 66-1
alert groups 66-6
configuring e-mail options 66-9
contact information 66-4
default settings 66-18
destination profiles 66-5
displaying information 66-14
mail-server priority 66-10
pattern matching 66-9
periodic notification 66-8
rate limit messages 66-9
severity threshold 66-8
smart call home feature 66-2
SMTP server 66-9
testing communications 66-10
call home alert groups
configuring 66-6
description 66-6
subscribing 66-7
call home contacts
assigning information 66-4
call home destination profiles
attributes 66-5
configuring 66-5
description 66-5
displaying 66-16
call home notifications
full-txt format for syslog 66-25
XML format for syslog 66-28
candidates
automatic discovery 15-7
candidate switch, cluster
defined 15-12
capture filter, Wireshark 57-7
capture points, Wireshark 57-6
Capturing control packets
selecting mode 52-7
cautions
Unicast RPF
BGP optional attributes 35-4
cautions for passwords
encrypting 3-22
CDP
automatic discovery in communities 15-7
configuration 29-2
defined with LLDP 30-1
displaying configuration 29-3
enabling on interfaces 29-3
host presence detection 45-8
Layer 2 protocol tunneling 28-13
maintaining 29-3
monitoring 29-3
overview 1-3, 29-1
cdp enable command 29-3
CEF
adjacency tables 34-2
and NSF with SSO 12-5
configuring load balancing 34-7
displaying statistics 34-8

enabling 34-6, 69-2
hardware switching 34-4
load balancing 34-6
overview 34-1
software switching 34-4
certificate authority (CA) 66-3
CFM
and Ethernet OAM, configuring 64-51
and Ethernet OAM interaction 64-51
clearing 64-31
configuration guidelines 64-7, 65-4
configuring crosscheck for VLANs 64-11
configuring fault alarms 64-16
configuring port MEP 64-14
configuring static remote MEP 64-13, 64-16, 64-18
crosscheck 64-5
defined 64-2
EtherChannel support 64-7, 65-4
fault alarms
configuring 64-16
IP SLAs support for 64-6
IP SLAs with endpoint discovers 64-21
maintenance domain 64-2
manually configuring IP SLAs ping or jitter 64-19
measuring network performance 64-6
monitoring 64-32, 64-33
port MEP, configuring 64-14
remote MEPs 64-5
static RMEP, configuring 64-13, 64-16, 64-18
static RMEP check 64-5
Y.1731
described 64-27
CGMP
overview 26-2
Change of Authorization, RADIUS 45-97
channel-group group command 5-46, 25-8, 25-10
Cisco 7600 series Internet router
enabling SNMP 71-4, 71-5
Cisco Discovery Protocol
See CDP
Cisco Express Forwarding
See CEF
Cisco Group Management Protocol
See CGMP
Cisco IOS IP SLAs 67-2
Cisco IOS NSF-aware
support 12-2
Cisco IOS NSF-capable support 12-2
Cisco IP Phones
configuring 42-3
sound quality 42-1
Cisco TrustSec
credentials 44-10
switch-to-switch security
802.1x mode 44-11
configuration example 44-14
manual mode 44-12
Cisco TrustSec Network Device Admission Control
See NDAC
CiscoWorks 2000 61-4
CIST
description 21-22
civic location 30-3
class level, configure in a service policy 41-31, 41-65
class of service
See CoS
clear cdp counters command 29-4
clear cdp table command 29-3
clear counters command 8-36
clearing
Ethernet CFM 64-31
IP multicast table entries 36-28
clear ip eigrp neighbors command 33-19
CLI
accessing 2-2
backing out one level 2-5
getting commands 2-5
history substitution 2-4

managing clusters 15-13
modes 2-5
monitoring environments 56-1
ROM monitor 2-7
software basics 2-4
client processes, tracking 58-1
clients
in 802.1X authentication 45-3
clock
See system clock
clustering switches
command switch characteristics
and VTY 15-12
convert to a community 15-10
managing
through CLI 15-13
overview 15-2
planning considerations
CLI 15-13
passwords 15-8
CoA Request Commands 45-100
command-line processing 2-3
command modes 2-5
commands
b 72-3
b flash 72-3
boot 72-3
confreg 72-3
dev 72-3
dir device 72-3
frame 72-5
i 72-3
listing 2-5
meminfo 72-5
reset 72-3
ROM monitor 72-2 to 72-3
ROM monitor debugging 72-5
SNMP 71-4
sysret 72-5
command switch, cluster
requirements 15-11
common and internal spanning tree
See CIST
common spanning tree
See CST
community of switches
access modes in Network Assistant 15-9
adding devices 15-9
communication protocols 15-8
community name 15-8
configuration information 15-9
converting from a cluster 15-10
host name 15-8
passwords 15-8
community ports 43-3
community strings
configuring 61-7
overview 61-4
community VLANs 43-2, 43-3
configure as a PVLAN 43-15
compiling MIBs 71-4
config-register command 3-29
config terminal command 3-9
configurable leave timer,IGMP 26-4
configuration examples
SNMP 61-15
configuration files
limiting TFTP server access 61-15
obtaining with DHCP 3-6
saving 3-10
system contact and location information 61-14
configuration guidelines
CFM 64-7, 65-4
Ethernet OAM 64-35
REP 23-7
SNMP 61-6
VLAN mapping 28-10
configuration register

boot fields
listing value 3-29
modifying 3-28
changing from ROM monitor 72-3
changing settings 3-28 to 3-29
configuring 3-26
settings at startup 3-27
configure class-level queue-limit in a service policy 41-31, 41-65
configure terminal command 3-29, 8-2
configuring access-group mode on Layer 2 interface 52-31
configuring flow control 8-23
configuring interface link and trunk status envents 8-37
configuring named IPv6 ACLs 52-16
configuring named MAC extended ACLs 52-14, 52-15
configuring unicast MAC address filtering 52-13
configuring VLAN maps 52-17
confreg command 72-3
Connectivity Fault Management
See CFM
console configuration mode 2-5
console download 72-4 to 72-5
console port
disconnecting user sessions 9-7
monitoring user sessions 9-6
contact information
assigning for call home 66-4
controlling switch access with RADIUS 45-95
Control Plane Policing
and Layer 2 Control packet QoS, configuration example 49-14
configuration guidelines and restrictions 49-8
configuring for control plane traffic 49-4
configuring for data plane and management plan traffic 49-5
defaults 49-4
general guidelines 49-3
monitoring 49-9
understanding 49-2
control protocol, IP SLAs 67-4
convergence
REP 23-4
copy running-config startup-config command 3-10
copy system:running-config nvram:startup-config command 3-32
core system filter, Wireshark 57-6
CoS
definition 41-3
figure 41-2
overriding on Cisco IP Phones 42-5
priority 42-5
counters
clearing MFIB 36-28
clearing on interfaces 8-36
CPU, impact of ACL processing 52-12
CPU port sniffing 56-10
crashfiles information, archiving 2-8
Critical Authentication
configure with 802.1X 45-62
crosscheck, CFM 64-5, 64-11
CST
description 21-25
IST and 21-22
MST and 21-22
customer edge devices 40-2
C-VLAN 1-2, 28-7

D

database agent
configuration examples 51-15
enabling the DHCP Snooping 51-13
daylight saving time 4-13
debug commands, ROM monitor 72-5
decoding and displaying packets, Wireshark 57-9
default configuration
802.1X 45-27
banners 4-24

DNS 4-23
Ethernet OAM 64-35
IGMP filtering 26-30
IGMP snooping 27-5, 27-6
IP SLAs 67-6
IPv6 53-7
Layer 2 protocol tunneling 28-16
LLDP 30-5
MAC address table 4-30
MVR 26-23
NTP 4-4
private VLANs 43-12
RADIUS 45-103
REP 23-7
resetting the interface 8-40
RMON 67-3
SNMP 61-5
SPAN and RSPAN 56-6
system message logging 59-3
TACACS+ 3-18
VLAN mapping 28-9
Y.1731 64-29
default gateway
configuring 3-11
verifying configuration 3-11
default settings, erase commad 3-32
default web-based authentication configuration
802.1X 47-6
defining/modifying/deleting a capture point, Wireshark 57-12
denial-of-service attacks
IP address spoofing, mitigating 35-5
Unicast RPF, deploying 35-5
denying access to a server on another VLAN 52-23
deploying 10-Gigabit Ethernet and a Gigabit Ethernet SFP ports 8-12, 8-13
deploying 10-Gigabit Ethernet and a Gigabit Ethernet SFP ports on WS-X4606-10GE-E and Sup 6-E 8-13
description command 8-23
dev command 72-3
device discovery protocol 30-1
device IDs
call home format 66-21, 66-22
device sensor
configuring 45-118
DHCP
configuring
rate limit for incoming packets 51-13
denial-of-service attacks, preventing 51-13
rate limiting of packets
configuring 51-13
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
identifying a port with 37-4
overview 51-4
DHCP Snooping
enabling, and Option 82 51-10
DHCP snooping
accepting untrusted packets form edge switch 51-10
configuring 51-6
default configuration 51-7
displaying binding tables 51-19
displaying configuration 51-19
displaying information 51-18
enabling 51-7
enabling on private VLAN 51-12

enabling on the aggregation switch 51-9
enabling the database agent 51-13
message exchange process 51-4
monitoring 51-23
option 82 data insertion 51-4
overview 51-1
Snooping database agent 51-2
DHCP Snooping Database Agent
adding to the database (example) 51-18
enabling (example) 51-15
overview 51-2
reading from a TFTP file (example) 51-17
Diagnostics
online 69-1
Power-On-Self-Test
causes of failure 69-20
how it works 69-10
overview 69-10
Power-On-Self-Test for Supervisor Engine V-10GE 69-13
Differentiated Services Code Point values
See DSCP values
DiffServ architecture, QoS 41-2
Digital optical monitoring transceiver support 8-19
dir device command 72-3
disabled state
RSTP comparisons (table) 21-24
disabling
broadcast storm control 55-5
disabling multicast storm control 55-5
disconnect command 9-7
discovery, clusters
See automatic discovery
discovery, Ethernet OAM 64-34
display dection and removal events 14-7
display filter, Wireshark 57-7
displaying
Auth Manager sumary for an interface 45-126
MAB details 45-128
summary of all Auth manager sessions 45-126
summary of all Auth manager sessions on the switch authorized for a specified authentication method 45-126
displaying EtherChannel to a Virtual Switch System 25-16
displaying storm control 55-6
displaying Wireshark information 57-14
display PoE consumed by a module 14-8
display PoE detection and removal events 14-7
DNS
and DHCP-based autoconfiguration 3-5
default configuration 4-23
displaying the configuration 4-24
overview 4-22
setting up 4-23
domain names
DNS 4-22
Domain Name System
See DNS
double-tagged packets
802.1Q tunneling 28-2
Layer 2 protocol tunneling 28-15
downloading MIBs 71-3, 71-4
drop threshold for Layer 2 protocol packets 28-16
DSCP values
definition 41-4
IP precedence 41-2
Dual_Active Detection
using Enhanced PAgP 5-23
Dual-Active Detection, using Fast-Hello 5-24
duplex command 8-22
duplex mode
configuring interface 8-20
dynamic ARP inspection
ARP cache poisoning 50-2
configuring
ACLs for non-DHCP environments 50-11
in DHCP environments 50-5
log buffer 50-14

rate limit for incoming ARP packets 50-16
denial-of-service attacks, preventing 50-16
interface trust state, security coverage 50-3
log buffer
configuring 50-14
logging of dropped packets 50-4
overview 50-1
port channels, their behavior 50-5
priority of static bindings 50-4
purpose of 50-2
rate limiting of ARP packets 50-4
configuring 50-16
validation checks, performing 50-19
Dynamic Host Configuration Protocol snooping
See DHCP snooping
dynamic port VLAN membership
example 16-29
limit on hosts 16-28
reconfirming 16-26
troubleshooting 16-28

E

EAP frames
changing retransmission time 45-85
exchanging (figure) 45-4, 45-6, 45-13
request/identity 45-4
response/identity 45-4
setting retransmission number 45-86
EAPOL frames
802.1X authentication and 45-3
OTP authentication, example (figure) 45-4, 45-13
start 45-4
Echo mode,configuring BFD 38-15
edge ports
description 21-27
EGP
overview 1-17
EIGRP
configuration examples 33-19
monitoring and maintaining 33-19
EIGRP (Enhanced IGRP)
stub routing
benefits 33-17
configuration tasks 33-18
configuring 33-14
overview 33-14
restrictions 33-17
verifying 33-18
EIGRP (enhanced IGRP)
overview 1-17
eigrp stub command 33-18
EIGRP stub routing, configuring 33-13
ELIN location 30-3
e-mail addresses
assigning for call home 66-4
e-mail notifications
Call Home 1-24, 66-2
Embedded CiscoView
displaying information 4-48
installing and configuring 4-45
overview 4-45
emergency alarms on Sup Engine 6-E systems 13-5
enable command 3-9, 3-28
enable mode 2-5
enabling SNMP 71-4, 71-5
encryption keying 44-2
encryption keys, MKA 44-2
Enhanced Interior Gateway Routing Protocol
See EIGRP
enhanced object tracking
defined 58-1
IP routing state 58-2
line-protocol state 58-2
tracked lists 58-3
Enhanced PoE support on E-series 14-15
Enhanced PoE support on E-series,configuring Universal PoE 14-16

environmental monitoring
using CLI commands 13-1
EPM logging 45-129
errdisable recovery
configuring 14-14
EtherChannel
channel-group group command 5-46, 25-8, 25-10
configuration guidelines 5-30, 25-5
configuring 25-6 to 25-16
configuring (tasks) 5-30
configuring Layer 2 25-10
configuring Layer 3 25-7
DFC restriction, see CSCdt27074 in the Release Notes
displaying to a virtual switch system 25-16
interface port-channel command 25-7
lacp system-priority
command example 25-13
modes 25-3
overview 25-2
PAgP
Understanding 25-4
physical interface configuration 5-46, 25-7
port-channel interfaces 25-2
port-channel load-balance command 25-14
removing 25-15
removing interfaces 25-15
understanding 5-2
EtherChannel guard
disabling 24-6
enabling 24-6
overview 24-6
Ethernet management port
and routing 8-6
and routing protocols 8-6
configuring 8-10
default setting 8-6
described 1-29, 8-6
for network management 1-29, 8-6
specifying 8-10
supported features 8-10
unsupported features 8-10
Ethernet management port, internal
and routing protocols 8-6
Ethernet Management Port, using 8-6
Ethernet OAM 64-34
and CFM interaction 64-51
configuration guidelines 64-35
configuring with CFM 64-51
default configuration 64-35
discovery 64-34
enabling 64-36, 64-52
link monitoring 64-34, 64-38
messages 64-34
protocol
defined 64-33
monitoring 64-49
remote failure indications 64-34
remote loopback 64-34, 64-37
templates 64-45
Ethernet OAM protocol CFM notifications 64-51
Ethernet Remote Defect Indication (ETH-RDI) 64-28
event triggers, user-defined
configuring, 802.1X-based 20-8
configuring, MAC address-based 20-9
explicit host tracking
enabling 26-11
extended range VLANs
See VLANs
Extensible Authentication Protocol over LAN 45-2
Exterior Gateway Protocol
See EGP

F

Fa0 port
See Ethernet management port
Failure detection, using BFD 38-7
Fallback Authentication

configure with 802.1X 45-77
FastDrop
overview 36-11
fastethernet0 port
See Ethernet management port
Fast-Hello
dual-active detection 5-24
Fast-Hello dual-active detection, configuring 5-50
fast link notification
on VSL failure 5-14
Fast UDLD
configuring probe message interval 31-8
default configuration 31-4
displaying link status 31-9
enabling globally 31-5
enabling on individual interface 31-7
enabling per-interface 31-6
modes of operation 31-3
resetting disabled LAN interfaces 31-8
use case 31-2
Fast UDLD, overview 31-1
feature interactions, Wireshark 57-10
FIB
description 34-2
See also MFIB
fiber-optics interfaces
disabling UDLD 31-7
Filter-ID ACL and Per-User ACL, configureport-based authentication
configure Per-User ACL and Filter-ID ACL 45-45
filtering
in a VLAN 52-18
non-IP traffic 52-14, 52-15
filters, Wireshark 57-6
flags 36-12
Flash memory
configuring router to boot from 3-31
loading system images from 3-30
security precautions 3-31
Flexible NetFlow
caveats 63-1, 63-7
defined 1-4, 63-1
Flex Links
configuration guidelines 22-6
configuring 22-6, 22-7
configuring preferred VLAN 22-9
configuring VLAN load balancing 22-8
monitoring 22-12
flooded traffic, blocking 54-2
flowchart, traffic marking procedure 41-21, 41-55
flow control, configuring 8-23
For 14-13
forward-delay time (STP)
configuring 21-19
forwarding information base
See FIB
frame command 72-5

G

gateway
See default gateway
get-bulk-request operation 61-3
get-next-request operation 61-3, 61-4
get-request operation 61-3, 61-4
get-response operation 61-3
Gigabit Ethernet SFP ports
deploy with 10-Gigabit Ethernet 8-12, 8-13
GLBP, introduction 1-15
global configuration mode 2-5
Guest-VLANs
configure with 802.1X 45-57

H

hardware and software ACL support 52-6
hardware switching 34-5

hello time (STP)
configuring 21-17
high CPU due to ACLs, troubleshooting 52-6
history
CLI 2-4
history table, level and number of syslog messages 59-9
hop counts
configuring MST bridges 21-28
host
limit on dynamic port 16-28
host modes, MACsec 44-3
host ports
kinds of 43-4
host presence CDP message 45-8
Hot Standby Routing Protocol
See HSRP
HSRP
description 1-16
HSRP, introduction 1-16
hw-module module num power command 13-22

I

ICMP
enabling 9-12
ping 9-7
running IP traceroute 9-9
time exceeded messages 9-9
ICMP Echo operation
configuring 67-11
IP SLAs 67-11
i command 72-3
IDS
using with SPAN and RSPAN 56-2
IEEE 802.1ag 64-2
IEEE 802.1s
See MST
IEEE 802.1w
See MST
IEEE 802.3ad
See LACP
IGMP
configurable-leave timer 26-4
description 36-3
enabling 36-14
explicit host tracking 26-4
immediate-leave processing 26-3
leave processing, enabling 27-8
overview 26-2
report suppression
disabling 27-10
IGMP filtering
configuring 26-31
default configuration 26-30
described 26-30
monitoring 26-34
IGMP groups
setting the maximum number 26-33
IGMP Immediate Leave
configuration guidelines 26-9
IGMP profile
applying 26-32
configuration mode 26-31
configuring 26-31
IGMP Snooping
configure
leave timer 26-9
configuring
Learning Methods 26-7
static connection to a multicast router 26-8
configuring host statically 26-11
enabling
Immediate-Leave processing
explicit host tracking 26-11
suppressing multicast flooding 26-12
IGMP snooping
configuration guidelines 26-5
default configuration 27-5, 27-6

enabling
globally 26-6
on a VLAN 26-6
enabling and disabling 27-6
IP multicast and 36-4
monitoring 26-14, 27-10
overview 26-2
IGMP Snooping, displaying
group 26-16
hot membership 26-15
how to 26-15
MAC address entries 26-18
multicast router interfaces 26-17
on a VLAN interface 26-18
Querier information 26-19
IGMPSnooping Querier, configuring 26-10
Immediate Leave, IGMP
enabling 27-8
immediate-leave processing
enabling 26-8
IGMP
See fast-leave processing
ingress packets, SPAN enhancement 56-12
inline power
configuring on Cisco IP phones 42-5
insufficient inline power handling for Supervisor Engine II-TS 13-22
Intelligent Power Management 14-4
interacting with Baby Giants 8-29
interface
displaying operational status 14-6
interface command 3-9, 8-2
interface configuration
REP 23-10
interface link and trunk status events
configuring 8-37
interface port-channel command 5-45, 25-7
interface range command 8-4
interface range macro command 8-11
interfaces
adding descriptive name 8-23
clearing counters 8-36
configuring 8-2
configuring ranges 8-4
displaying information about 8-36
Layer 2 modes 18-3
maintaining 8-35
monitoring 8-35
naming 8-23
numbers 8-2
overview 8-2
restarting 8-37
See also Layer 2 interfaces
using the Ethernet Management Port 8-6
Internet Control Message Protocol
See ICMP
Internet Group Management Protocol
See IGMP
Internet Protocol version 6
See IPv6
introduction
802.1X Identity-Based Network Security, list of supported features 1-34
Bidirectional Forwarding Detection 1-14
Cisco Call Home 1-24
Cisco Energy Wise 1-24
Cisco Express Forwarding 1-14
Cisco IOS IP Service Level Agreements 1-24
Cisco IOS Mediatrace and Performance Monitor 1-26
Cisco Medianet AutoQoS 1-25
Cisco Medianet Flow Metadata 1-26
Cisco Media Services Proxy 1-25
Cisco TrustSec MACsec Encryption 1-35
Cisco TrustSec Security Architecture 1-36
Debugging Features (platform and debug platform) 1-43
Device Sensor 1-14
Dynamic Host Control Protocol 1-28

Easy Virtual Network 1-28
EIGRP Stub routing 1-14
Embedded Event Manager 1-29
Enhanced Object Tracking 1-15
EtherChannel bundles 1-3
Ethernet CFM 1-3
Ethernet Management Port 1-29
Ethernet OAM Protocol 1-3
FAT File Management System (Sup 60-E, 6L-E, 4948E, and 4900M) 1-30
File System Management (Sup 7-E and 7L-E) 1-29
Flexible Netflow (Sup 7-E and 7L-E) 1-4
Flex Link and MAC Address-Table Move Update 1-4
GLBP 1-15
hard-based Control Plane Policing 1-37
HSRP 1-16
In Service Software Upgrade 1-19
Intelligent Power Management 1-30
Internet Group Management Protocol (IGMP) Snooping 1-4
IP Routing protocols 1-17
IP Source Guard 1-38
IP Source Guard or Static Hosts 1-38
IPv6 1-19
IPv6 First Hop Security 1-38
IPv6 Multicast BSR and BSR Scoped Zone Support, introduction 1-5
IPv6 Multicast Listen Discovery (MLD) and Multicast Listen Discovery Snooping 1-6
IS-IS 1-18
Jumbo Frame 1-6
Layer 2 traceroute 1-42
Link Aggregation Control Protocol 1-7
MAC Address Notification 1-30
NAC
  Layer 2 802.1X authentication 1-40
  Layer 2 IP validation 1-40
NetFlow-lite 1-30
Network Security with ACLs (IP ACLs, MAC ACLs, Port ACLs, Router, ACLs, and VLAN ACLs) 1-40
NSF with SSO 1-20
OSPF 1-18
OSPF for Routed Access 1-21
Port Security 1-41
Power over Ethernet 1-31
RIP 1-19
Simple Network Management Protocol 1-31
SPAN and RSPAN 1-32
Time Domain Reflectometry 1-43
Unicast Reverse Path Forwarding 1-22
Universal Power over Ethernet 1-32
Virtual Router Redundancy Protocol 1-22
VRF-lite 1-22
Web-based Authentication 1-43
Web Content Coordination Protocol 1-32
Wireshark 1-33
XML-PI 1-33
Intrusion Detection System
  See IDS
inventory management TLV 30-3, 30-9
IOS shell
  See Auto SmartPorts macros
IP
  configuring default gateway 3-11
  configuring static routes 3-11
  displaying statistics 34-8
IP addresses
  128-bit 53-2
  cluster candidate or member 15-12
  cluster command switch 15-11
  discovering 4-44
  IPv6 53-2
ip cef command 34-6, 69-2
IP Enhanced IGRP
  interfaces, displaying 33-19
ip icmp rate-limit unreachable command 9-12
ip igmp profile command 26-31
ip igmp snooping tcn flood command 26-13
ip igmp snooping tcn flood query count command 26-14

ip igmp snooping tcn query solicit command 26-14
IP information
assigned
through DHCP-based autoconfiguration 3-2
ip load-sharing per-destination command 34-7
ip local policy route-map command 39-11
ip mask-reply command 9-13
IP MTU sizes,configuring 33-9
IP multicast
clearing table entries 36-28
configuring 36-13
default configuration 36-13
displaying PIM information 36-23
displaying the routing table information 36-24
enabling dense-mode PIM 36-15
enabling sparse-mode 36-15
features not supported 36-13
hardware forwarding 36-9
IGMP snooping and 26-5, 36-4
overview 36-1
routing protocols 36-2
software forwarding 36-9
See also Auto-RP; IGMP; PIM; RP; RPF
IP multicast routing
enabling 36-14
monitoring and maintaining 36-23
ip multicast-routing command 36-14
IP multicast traffic, load splitting 36-22
IP phones
configuring voice ports 42-3
See Cisco IP Phones 42-1
ip pim command 36-15
ip pim dense-mode command 36-15
ip pim sparse-dense-mode command 36-16
ip policy route-map command 39-8, 39-10
IP Port Security for Static Hosts
on a Layer 2 access port 51-25
on a PVLAN host port 51-28
overview 51-24
ip redirects command 9-13
IP routing tables
deleting entries 36-28
IP Service Level Agreements
See IP SLAs
IP service levels, analyzing 67-1
IP SLAs
benefits 67-2
CFM endpoint discovery 64-21
configuration guidelines 67-6
Control Protocol 67-4
default configuration 67-6
definition 67-1
ICMP echo operation 67-11
manually configuring CFM ping or jitter 64-19
measuring network performance 67-3
multioperations scheduling 67-5
operation 67-3
reachability tracking 58-9
responder
described 67-4
enabling 67-7
response time 67-4
scheduling 67-5
SNMP support 67-2
supported metrics 67-2
threshold monitoring 67-6
track state 58-9
UDP jitter operation 67-8
IP Source Guard
configuring 51-20
configuring on private VLANs 51-22
displaying 51-22, 51-23
overview 51-23
IP statistics
displaying 34-8
IP traceroute
executing 9-9
overview 9-8

IP unicast
displaying statistics 34-8
IP Unnumbered support
configuring on a range of Ethernet VLANs 17-5
configuring on LAN and VLAN interfaces 17-4
configuring with connected host polling 17-6
DHCP Option 82 17-2
displaying settings 17-7
format of agent remote ID suboptions 17-2
troubleshooting 17-8
with conected host polling 17-3
with DHCP server and Relay agent 17-2
ip unreachables command 9-12
IPv4, IPv6, and MAC ACLs, configuring on a Layer 2 interface 52-29
IPv6
addresses 53-2
default configuration 53-7
defined 1-19, 53-1
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 53-6
Router ID 53-6
OSPF 53-6
IPv6 control traffic, policing 49-16
IPv6 First Hop Security, introduction 1-38
IPX
redistribution of route information with EIGRP 1-17
is 28-19
IS-IS, introduction 1-18
ISL
trunking with 802.1Q tunneling 28-4
isolated port 43-4
isolated VLANs 43-2, 43-3, 43-4
ISSU
compatibility matrix 5-59, 6-14, 7-13
compatiblity verification using Cisco Feature Navigator 5-60, 6-15, 7-14
NSF overview 6-3, 7-3
perform the process
aborting a software upgrade 5-76, 6-34, 7-33
configuring the rollback timer as a safeguard 5-77, 6-35, 7-35
displaying a compatibility matrix 5-79, 6-36, 6-40, 7-36
loading the new software on the new standby 5-69, 6-27, 7-26
stopping the rollback timer 5-68, 6-26, 7-25
switching to the standby 5-66, 6-24, 7-23
verify the ISSU state 5-63, 6-20, 7-20
verify the redundancy mode 5-62, 6-19, 7-18
verify the software installation 5-61, 6-18, 7-18
vload the new software on standby 5-65, 6-21, 7-20
prerequisites 5-55, 6-2, 7-2
process overview 6-6, 7-6
restrictions 5-55, 6-2, 7-2
SNMP support 6-15, 7-14
SSO overview 6-3, 7-3
versioning capability in software to support 6-13
IST
and MST regions 21-22
description 21-22
master 21-27
ITU-T Y.1731
See Y.1731

J

jumbo frames
and ethernet ports 8-27
configuring MTU sizes for 8-28
ports and linecards that support 8-26
understanding MTUs 8-26
understanding support 8-26
VLAN interfaces 8-28

K

keyboard shortcuts 2-3

L

l2protocol-tunnel command 28-17
labels, definition 41-3
LACP
  system ID 25-4
Layer 2 access ports 18-7
Layer 2 Control Packet QoS
  and CoPP configuration example 49-14
  default configuation 49-11
  disabling 49-13
  enabvling 49-12
  guideline and restrictions 49-16
  understanding 49-11
Layer 2 frames
  classification with CoS 41-2
Layer 2 interface
  applying ACLs 52-31
  configuring access-mode mode on 52-31
  configuring IPv4, IPv6, and MAC ACLs 52-29
  displaying an ACL configuration 52-32
Layer 2 interfaces
  assigning VLANs 16-7
  configuring 18-5
  configuring as PVLAN host ports 43-18
  configuring as PVLAN promiscuous ports 43-17
  configuring as PVLAN trunk ports 43-19
  defaults 18-4
  disabling configuration 18-8
  modes 18-3
  show interfaces command 18-6
Layer 2 interface type
  resetting 43-24
  setting 43-24
Layer 2 protocol tunneling
  default configuration 28-16
  guidelines 28-16
Layer 2 switching
  overview 18-1
Layer 2 Traceroute
  and ARP 9-10
  and CDP 9-10
  host-to-host paths 9-10
  IP addresses and subnets 9-10
  MAC addresses and VLANs 9-10
  multicast traffic 9-10
  multiple devices on a port 9-10
  unicast traffic 1-42, 9-9
  usage guidelines 9-10
Layer 2 trunks
  configuring 18-5
  overview 18-3
Layer 3 interface, applying IPv6 ACLs 52-17
Layer 3 interface counters,configuring 33-10
Layer 3 interface counters,understanding 33-3
Layer 3 interfaces
  changing from Layer 2 mode 40-16
  configuration guidelines 33-5
  configuring VLANs as interfaces 33-7
  overview 33-1
    counters 33-3
    logical 33-2
    physical 33-2
    SVI autostate exclude 33-3
Layer 3 packets
  classification methods 41-2
Layer 4 port operations
  configuration guidelines 52-11
  restrictions 52-10
Leave timer, enabling 26-9
licenses, managing with PRTU 4-14
limitations on using a TwinGig Convertor 8-14
Link Aggregation Control Protocol, introduction 1-7
link and trunk status events
  configuring interface 8-37
link integrity, verifying with REP 23-4
Link Layer Discovery Protocol
  See CDP

link monitoring, Ethernet OAM 64-34, 64-38
link-state tracking
configuration guidelines 25-21
default configuration 25-21
described 25-18
displaying status 25-22
generic configuration procedure 25-21
link status, displaying UDLD 31-9
listening state (STP)
RSTP comparisons (table) 21-24
LLDP
configuring 30-4
characteristics 30-5
default configuration 30-5
disabling and enabling
globally 30-6
on an interface 30-7
monitoring and maintaining 30-14
overview 30-1
transmission timer and holdtime, setting 30-5
LLDP-MED
configuring
procedures 30-4
TLVs 30-9, 30-11
monitoring and maintaining 30-14
overview 30-1
supported TLVs 30-2
LLDP Media Endpoint Discovery
See LLDP-MED
load balancing
configuring for CEF 34-7
configuring for EtherChannel 25-14
overview 25-5, 34-6
per-destination 34-7
load splitting IP multicast traffic 36-22
Location Service
overview 30-1
location service
configuring 30-12
understanding 30-3
location TLV 30-3, 30-9
logging, EPM 45-129
Logical Layer 3 interfaces
configuring 33-6
logical layer 3 VLAN interfaces 33-2
login authentication
with RADIUS 45-106
with TACACS+ 3-19
login banners 4-24
login timer
changing 9-6
logoutwarning command 9-6
loop guard
and MST 21-23
configuring 24-4
overview 24-3

M

MAC/PHY configuration status TLV 30-2
MAC addresses
aging time 4-30
allocating 21-6
and VLAN association 4-29
building tables 4-28, 18-2
convert dynamic to sticky secure 48-5
default configuration 4-30
disabling learning on a VLAN 4-39
discovering 4-44
displaying 9-3
displaying in DHCP snooping binding table 51-19
dynamic
learning 4-29
removing 4-31
in ACLs 52-14
static
adding 4-37
allowing 4-38

characteristics of 4-36
dropping 4-38
removing 4-37
sticky 48-4
sticky secure, adding 48-5
MAC address learning, disabling on a VLAN 4-39
confuguring 4-39
deployment scenarios 4-40
feature compatibility 4-42
feature incompatibility 4-43
feature inompatibility 4-43
usage guidelines 4-40
MAC address table
displaying 4-44
MAC address-table move update
configuration guidelines 22-10
configuring 22-10
monitoring 22-12
MAC Authentication Bypass
configure with 802.1X 45-60
MAC details, displaying 45-128
MAC extended access lists 52-14
macl 52-14
macros
See Auto SmartPorts macros
See Auto Smartports macros
See Smartports macros
MACSec
802.1AE Tagging 44-9
MACsec 44-2
configuring on an interface 44-7
defined 44-1, 44-2
switch-to-switch security 44-1
MACsec Key Agreement Protocol
See MKA
main-cpu command 10-8, 11-7
management address TLV 30-2
management options
SNMP 61-1
Management Port, Ethernet 8-6
managing software licenses, using PRTU 4-14
manual preemption, REP, configuring 23-13
marking
hardware capabilities 41-23, 41-57
marking action drivers 41-21, 41-55
marking network traffic 41-18, 41-52
marking support, multi-attribute 41-22, 41-56
match ip address command 39-6, 39-9
maximum aging time (STP)
configuring 21-18
MDA
configuration guidelines 45-23 to ??
described 45-23
MEC
configuration 5-45
described 5-14
failure 5-15
Media Access Control Security
See MACsec
members
automatic discovery 15-7
member switch
managing 15-13
member switch, cluster
defined 15-2
meminfo command 72-5
messages, Ethernet OAM 64-34
messages, to users through banners 4-24
Metro features
Y.1731 (AIS and RDI), introduction 1-12
metro tags 28-2
MFIB
CEF 36-6
overview 36-12
MFIB, IP
displaying 36-26
MIBs
compiling 71-4

downloading 71-3, 71-4
overview 61-1
related information 71-3
SNMP interaction with 61-4
MKA
configuring policies 44-6
defined 44-2
policies 44-2
replay protection 44-3
statistics 44-4
virtual ports 44-3
MLD Done messages and Immediate-leave 27-4
MLD messages 27-2
MLD queries 27-3
MLD reports 27-4
MLD Snooping
MLD Done messages and Immediate-leave 27-4
MLD messages 27-2
MLD queries 27-3
MLD reports 27-4
Multicast client aging robustness 27-3
Multicast router discovery 27-3
overview 27-1
Mode of capturing control packets, selecting 52-7
modules
checking status 9-1
powering down 13-22
monitoring
802.1Q tunneling 28-18
ACL information 52-35
Ethernet CFM 64-32, 64-33
Ethernet OAM 64-49
Ethernet OAM protocol 64-49
Flex Links 22-12
IGMP
snooping 27-10
IGMP filters 26-34
IGMP snooping 26-14
Layer 2 protocol tunneling 28-18
MAC address-table move update 22-12
multicast router interfaces 27-11
multi-VRF CE 40-14, 40-21, 40-22
MVR 26-29
object tracking 58-12
REP 23-14
traffic flowing among switches 67-1
tunneling 28-18
VLAN filters 52-24
VLAN maps 52-24
monitoring and troubleshooting
BFD 38-17
M-record 21-23
MST
and multiple spanning trees 1-8, 21-22
boundary ports 21-27
BPDUs 21-23
configuration parameters 21-26
configuring 21-29
displaying configurations 21-33
edge ports 21-27
enabling 21-29
hop count 21-28
instances
configuring parameters 21-32
description 21-23
number supported 21-26
interoperability with PVST+ 21-23
link type 21-28
master 21-27
message age 21-28
regions 21-26
restrictions 21-29
to-SST interoperability 21-24
MSTP
EtherChannel guard
enabling 24-6
M-record 21-23
M-tree 21-23

M-tree 21-23
MTUS
understanding 8-26
MTU size
configuring 8-28, 8-29, 8-38
default 16-5
Multi-authentication
described 45-23
multiauthentication mode 45-8
multicast
See IP multicast
Multicast client aging robustness 27-3
multicast Ethernet loopback, using 64-31
multicast Ethernet loopback (ETH-LB) 64-29
Multicast Forwarding Information Base (MFIB) 36-12
multicast groups
static joins 27-7
Multicast HA 36-13
Multicast implementation
HA 36-13
MFIB 36-12
S/M, 224/4 36-13
multicast packets
blocking 54-2
Multicast router discovery 27-3
multicast router interfaces, displaying 26-17
multicast router interfaces, monitoring 27-11
multicast router ports, adding 27-7
multicast routers
flood suppression 26-12
multicast router table
displaying 36-24
Multicast Storm Control
enabling 55-4
disabling 55-5
multicast television application, using MVR 26-21
Multicast VLAN Registration
See MVR
multichassis EtherChannel
see MEC 5-14
multidomain authentication
See MDA
multidomain authentication mode 45-7
multioperations scheduling, IP SLAs 67-5
Multiple AuthorizationAuthentication
configuring 45-34
Multiple Domain Authentication 45-34
multiple forwarding paths 1-8, 21-22
multiple-hosts mode 45-7
Multiple Spanning Tree
See MST
multiple VPN routing/forwarding
See multi-VRF CE
multi-VRF CE
components 40-3
configuration example 40-17
defined 40-1
displaying 40-14, 40-21, 40-22
monitoring 40-14, 40-21, 40-22
network components 40-3
packet-forwarding process 40-3
MVR
configuration guidelines and limitations 26-23
configuring global parameters 26-24
configuring on access ports 26-26
configuring on a trunk port 26-27
default configuration 26-23
displaying information 26-29
in a multicast television application 26-21
monitoring 26-29
setting global parameters 26-24

N

NAC Layer 2 802.1X authentication, intro 1-40
NAC Layer 2 IP validation, intro 1-40
named IPv6 ACLs, configuring

ACLs
configuring named IPv6 ACLs 52-16
named MAC extended ACLs
ACLs
configuring named MAC extended 52-14, 52-15
native VLAN
and 802.1Q tunneling 28-4
specifying 18-5
NDAC 44-9
defined 44-9
MACsec 44-1
NEAT
configuring 45-88
overview 45-24
neighbor offset numbers, REP 23-5
NetFlow-lite
clear commands 62-9
display commands 62-8
NetFlow packet sampling
about 62-2
Network Assistant
and VTY 15-12
configure
enable communication with switch 15-13, 15-17
default configuration 15-3
overview of CLI commands 15-3
Network Device Admission Control (NDAC) 44-9
Network Edge Access Topology
See NEAT
network fault tolerance 1-8, 21-22
network management
configuring 29-1
RMON 67-1
SNMP 61-1
network performance, measuring with IP SLAs 67-3
network policy TLV 30-2, 30-9
Network Time Protocol
See NTP
network traffic, marking 41-18, 41-52
New Software Features in Release 7.7
TDR 9-3
Next Hop Resolution Protocol
See NHRP
NHRP
support 1-18
non-fiber-optics interfaces
disabling UDLD 31-7
non-IP traffic filtering 52-14, 52-15
non-RPF traffic
description 36-10
in redundant configurations (figure) 36-11
Nonstop Forwarding
See NSF
nonvolatile random-access memory
See NVRAM
normal-range VLANs
See VLANs
NSF
defined 12-1
guidelines and restrictions 12-9
operation 12-4
NSF-aware
supervisor engines 12-3
support 12-2
NSF-capable
supervisor engines 12-3
support 12-2
NSF with SSO supervisor engine redundancy
and CEF 12-5
overview 12-3
SSO operation 12-4
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
ntroduction
PPPoE Intermediate Agent 1-41
Storm Control 1-42
uRPF Strict Mode 1-42
NVRAM
saving settings 3-10

O

OAM
client 64-34
features 64-34
sublayer 64-34
OAM manager
configuring 64-52
with CFM and Ethernet OAM 64-51
OAM PDUs 64-35
OAM protocol data units 64-33
OBFL, displaying for the 9000W AC 13-4
object tracking
monitoring 58-12
OIR
overview 8-33
on-demaind online diagnostics 69-2
online diagnostic
troubleshooting 69-8
Online Diagnostics 69-1
online diagnostics
configuring on-demaind 69-2
data path, displaying test results 69-7
displaying tests and test results 69-4
linecard 69-8
scheduling 69-2
starting and stopping tests 69-3
online insertion and removal
See OIR
Open Shortest Path First
See OSPF
operating system images
See system images
Option 82
enabling DHCP Snooping 51-10
OSPF
area concept 1-18
description 1-18
for IPv6 53-6
OSPF, introduction 1-18
OSPF for Routed Access, introduction 1-21

P

packets
modifying 41-9
packet type filtering
overview 56-14
SPAN enhancement 56-14
PACL
using with access-group mode 52-30
PACL configuration guidelines 52-28
PACL with VLAN maps and router ACLs 52-32
PAgP
understanding 25-4
PAgP, dual-active detection 5-23
passwords
configuring enable password 3-14
configuring enable secret password 3-14

encrypting 3-22
in clusters 15-8
recovering lost enable password 3-25
setting line password 3-14
PBR (policy-based routing)
configuration (example) 39-12
enabling 39-6, 39-9
features 39-2
overview 39-1
route-map processing logic 39-3
route-map processing logic example 39-4
route maps 39-2
when to use 39-5
percentage thresholds in tracked lists 58-6
Permanent Right-To_Use 4-14
per-port and VLAN Access Control List 51-19
per-port per-VLAN QoS
enabling 41-36, 41-70
overview 41-10
Per-User ACL and Filter-ID ACL, configure 45-45
Per-VLAN Rapid Spanning Tree 21-6
enabling 21-20
overview 21-6
PE to CE routing, configuring 40-9
physical layer 3 interfaces 33-2
Physical Layer 3 interfaces, configuring 33-12
PIM
configuring dense mode 36-15
configuring sparse mode 36-15
displaying information 36-23
displaying statistics 36-27
enabling sparse-dense mode 36-15, 36-16
overview 36-3
PIM-DM 36-3
PIM on an interface, enabling 36-14
PIM-SM 36-3
PIM-SSM mapping, enabling 36-17
ping
executing 9-8
overview 9-7
ping command 9-8, 36-23
PoE 14-7, 14-8
configuring power consumption, powered devices 14-5
configuring power consumption for single device 14-5, 14-16
displaying operational status for an interface 14-6
Enhanced PoE support on E-series 14-15
policing and monitoring 14-12
power consumption for powered devices
Intelligent Power Management 14-4
powering down a module 13-22
power management modes 14-2
PoE policing
configuring errdisable recovery 14-14
configuring on an interface 14-13
displaying on an interface 14-14
power modes 14-12
point-to-point
in 802.1X authentication (figure) 45-3
policing
how to implement 41-18, 41-52
See QoS policing
policing, PoE 14-12
policing IPv6 control traffic 49-16
policy associations, QoS on Sup 6-E 41-39, 41-73
policy-map command 41-16, 41-51
policy map marking action, configuring 41-23, 41-57
port ACLs
and voice VLAN 52-4
defined 52-3
Port Aggregation Protocol
see PAgP
port-based authentication
802.1X with voice VLAN 45-22
Authentication Failed VLAN assignment 45-17
authentication server
defined 47-2

changing the quiet period 45-84
client, defined 45-3, 47-2
configuration guidelines 45-29, 47-6
configure ACL assignments and redirect URLs 45-38
configure switch-to-RADIUS server communication 45-32
configure with Authentication Failed 45-70
configure with Critical Authentication 45-62
configure with Guest-VLANs 45-57
configure with MAC Authentication Bypass 45-60
configure with VLAN User Distribution 45-68
configure with Voice VLAN 45-72
configuring
  Multiple Domain Authentication and Multiple Authorization 45-34
  RADIUS server 47-10
  RADIUS server parameters on the switch 47-9
configuring Fallback Authentication 45-77
configuring Guest-VLAN 45-32
configuring manual re-authentication of a client 45-94
configuring with Unidirectional Controlled Port 45-66
controlling authorization state 45-5
default configuration 45-27, 47-6
described 45-1
device roles 45-2, 47-2
displaying statistics 45-125, 47-14
enabling 45-29
  802.1X authentication 47-9
enabling multiple hosts 45-83
enabling periodic re-authentication 45-81
encapsulation 45-3
host mode 45-6
how 802.1X fails on a port 45-25
initiation and message exchange 45-4
method lists 45-29
modes 45-6
multidomain authentication 45-23
multiple-hosts mode, described 45-7
port security
  multiple-hosts mode 45-7
ports not supported 45-5
pre-authentication open access 45-8
resetting to default values 45-95
setting retransmission number 45-86
setting retransmission time 45-85
switch
  as proxy 47-2
switch supplicant
  configuring 45-88
  overview 45-24
topologies, supported 45-26
using with ACL assignments and redirect URLs 45-20
using with port security 45-19
voice aware 802.1x security
  configuring 45-74
  described 45-22, 45-73
with Critical Authentication 45-14
with Guest VLANs 45-11
with MAC Authentication Bypass 45-12
with Unidirectional Controlled Port 45-15
with VLAN assignment 45-10
with VLAN User Distribution 45-16
port-channel
  see EtherChannel
port-channel interfaces
  See also EtherChannel
  creating 5-45, 25-7
  overview 25-2
port-channel load-balance
  command 25-13
  command example 25-13
port-channel load-balance command 25-14
port cost (STP)
  configuring 21-15
port description TLV 30-2
PortFast

and MST 21-23
BPDU filter, configuring 24-9
configuring or enabling 24-15
overview 24-6
PortFast BPDU filtering
and MST 21-23
enabling 24-9
overview 24-9
port numbering with TwinGig Convertors 8-13
port priority
configuring MST instances 21-32
configuring STP 21-13
ports
blocking 54-1
checking status 9-2
dynamic VLAN membership
example 16-29
reconfirming 16-26
forwarding, resuming 54-3
REP 23-6
See also interfaces
port security
aging 48-5
configuring 48-7
displaying 48-28
guidelines and restrictions 48-33
on access ports 48-7, 48-22
on private VLAN 48-14
host 48-14
promiscuous 48-16
topology 48-15, 48-18, 48-32
on trunk port 48-17
guidelines and restrictions 48-15, 48-18, 48-32
port mode changes 48-22
on voice ports 48-22
sticky learning 48-5
using with 802.1X 45-19
violations 48-6
with 802.1X Authentication 48-32
with DHCP and IP Source Guard 48-31
with other features 48-33
port states
description 21-5
port VLAN ID TLV 30-2
power
inline 42-5
power dc input command 13-21
powered devices, configuring power consumption 14-5
power handling for Supervisor Engine II-TS 14-12
power inline command 14-3
power inline consumption command 14-5
power management
Catalyst 4500 series 13-7
Catalyst 4500 Switch power supplies 13-14
Catalyst 4948 series 13-23
configuring combined mode 13-13
configuring redundant mode 13-12
overview 13-1
redundancy 13-7
power management for Catalyst 4500 Switch
combined mode 13-9
redundant mode 13-9
power management limitations in Catalyst 4500 Switch 13-10
power management mode
selecting 13-10
power management TLV 30-2, 30-3, 30-9
power negotiation
through LLDP 30-11
Power-On-Self-Test diagnostics 69-10, 69-20
Power-On-Self-Test for Supervisor Engine V-10GE 69-13
power policing, displaying on an interface 14-14
power redundancy-mode command 13-13
power supplies
available power for Catalyst 4500 Switch 13-14
fixed 13-8
variable 13-8, 13-23

pre-authentication open access 45-8
pre-authentication open access. See port-based authentication.
preempt delay time, REP 23-5
primary edge port, REP 23-4
primary VLANs 43-2, 43-4
  associating with secondary VLANs 43-16
  configuring as a PVLAN 43-15
priority
  overriding CoS of incoming frames 42-5
priority queuing, QoS on Sup 6-E 41-30, 41-64
private VLAN
  configure port security 48-14, 48-15
  enabling DHCP Snooping 51-12
private VLANs
  across multiple switches 43-5
  and SVIs 43-10
  benefits of 43-2
  community ports 43-3
  community VLANs 43-2, 43-3
  default configuration 43-12
  end station access to 43-3
  isolated port 43-4
  isolated VLANs 43-2, 43-3, 43-4
  ports
    community 43-3
    isolated 43-4
    promiscuous 43-4
  primary VLANs 43-2, 43-4
  promiscuous ports 43-4
  secondary VLANs 43-2
  subdomains 43-2
  traffic in 43-9
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 43-17
  defined 43-4
  setting mode 43-24
protocol timers 21-4
provider edge devices 40-2
PRTU, managing software licenses 4-14
pruning, VTP
  See VTP pruning
pseudobridges
  description 21-25
PVACL 51-19
PVID (port VLAN ID)
  and 802.1X with voice VLAN ports 45-22
PVLAN promiscuous trunk port
  configuring 43-11, 43-17, 43-21
PVLANs
  802.1q support 43-14
  across multiple switches 43-5
  configuration guidelines 43-12
  configure port security 48-14, 48-16, 48-18
  configure port security in a wireless setting 48-32
  configuring 43-11
  configuring a VLAN 43-15
  configuring promiscuous ports 43-17
  host ports
    configuring a Layer 2 interface 43-18
    setting 43-24
  overview 43-1
  permitting routing, example 43-23
  promiscuous mode
    setting 43-24
  setting
    interface mode 43-24

Q

QoS
  classification 41-6 to ??

definitions 41-3
enabling per-port per-VLAN 41-36, 41-70
overview 41-1
overview of per-port per-VLAN 41-10
packet modification 41-9
traffic shaping 41-9
See also COS; DSCP values; transmit queues
QoS active queue management
tracking queue length 41-9
QoS labels
definition 41-3
QoS marking
description 41-5
QoS on Sup 6-E
Active Queue management via DBL 41-34, 41-68
active queue management via DBL 41-27, 41-34, 41-61, 41-68
classification 41-16, 41-50
configuring 41-13, 41-47
configuring CoS mutation 41-45, 41-79
configuring the policy map marking action 41-23, 41-57
hardware capabilities for marking 41-23, 41-57
how to implement policing 41-18, 41-52
marking action drivers 41-21, 41-55
marking network traffic 41-18, 41-52
MQC-based QoS configuration 41-13, 41-48
multi-attribute marking support 41-22, 41-56
platform hardware capabilities 41-15, 41-49
platform restrictions 41-18, 41-52
platform-supported classification criteria and QoS features 41-13, 41-14, 41-48
policing 41-17, 41-51
policy associations 41-39, 41-73
prerequisites for applying a service policy 41-15, 41-49
priority queuing 41-30, 41-64
queue-limiting 41-31, 41-65
restrictions for applying a service policy 41-15, 41-50
shaping 41-25, 41-59
sharing(bandwidth) 41-27, 41-61
sharing(blandwidth), shapring, and priority queuing 41-25, 41-59
software QoS 41-40, 41-74
traffic marking procedure flowchart 41-21, 41-55
QoS policing
definition 41-5
described 41-8
QoS policy
attaching to interfaces 41-8
QoS service policy
prerequisites 41-15, 41-49
restrictions for applying 41-15, 41-50
QoS transmit queues
burst 41-9
maximum rate 41-9
sharing link bandwidth 41-9
quad-supervisor
uplink forwarding 5-6
Quality of service
See QoS
queueing 41-8
queue-limiting, QoS on Sup 6-E 41-31, 41-65

R

RADIUS
attributes
vendor-proprietary 45-114
vendor-specific 45-112
change of authorization 45-97
configuring
accounting 45-111
authentication 45-106
authorization 45-110
communication, global 45-104, 45-112
communication, per-server 45-103, 45-104
multiple UDP ports 45-104
default configuration 45-103
defining AAA server groups 45-108

displaying the configuration 45-116
identifying the server 45-103
limiting the services to the user 45-110
method list, defined 45-103
operation of 45-97
server load balancing 45-116
suggested network environments 45-96
tracking services accessed by user 45-111
understanding 45-96
RADIUS, controlling switch access with 45-95
RADIUS Change of Authorization 45-97
RADIUS server
configure to-Switch communication 45-32
configuring settings 45-34
parameters on the switch 45-32
RA Guard
configuring 52-36
deployment 52-36
examples 52-37
introduction 52-35
usage guidelines 52-38
range command 8-4
range macros
defining 8-11
ranges of interfaces
configuring 8-4
Rapid Spanning Tree
See RSTP
rcommand command 15-13
reachability, tracking IP SLAs IP host 58-9
re-authentication of a client
configuring manual 45-94
enabling periodic 45-81
redirect URLs, port-based authentication 45-20
reduced MAC address 21-2
redundancy
configuring 10-7, 11-7
guidelines and restrictions 10-5, 11-5
changes made through SNMP 10-11, 11-11
NSF-aware support 12-2
NSF-capable support 12-2
overview 10-2, 11-2
redundancy command 10-8, 11-7
understanding synchronization 10-4, 11-5
redundancy (NSF) 12-1
configuring
BGP 12-11
CEF 12-10
EIGRP 12-16
IS-IS 12-13
OSPF 12-12
routing protocols 12-5
redundancy (RPR)
route processor redundancy 10-2, 11-3
synchronization 10-5, 11-5
redundancy (SSO)
redundancy command 12-10
route processor redundancy 10-3, 11-3
synchronization 10-5, 11-5
reload command 3-28, 3-29
Remote Authentication Dial-In User Service
See RADIUS
remote failure indications 64-34
remote loopback, Ethernet OAM 64-34, 64-37
Remote Network Monitoring
See RMON
rendezvous point, configuring 36-17
rendezvous point, configuring single static 36-20
REP
administrative VLAN 23-8
administrative VLAN, configuring 23-9
and STP 23-6
configuration guidelines 23-7
configuring interfaces 23-10
convergence 23-4
default configuration 23-7
manual preemption, configuring 23-13
monitoring 23-14

neighbor offset numbers 23-5
open segment 23-2
ports 23-6
preempt delay time 23-5
primary edge port 23-4
ring segment 23-2
secondary edge port 23-4
segments 23-1
characteristics 23-2
SNMP traps, configuring 23-14
supported interfaces 23-1
triggering VLAN load balancing 23-6
verifying link integrity 23-4
VLAN blocking 23-13
VLAN load balancing 23-4
replication
description 36-9
report suppression, IGMP
disabling 27-10
reserved-range VLANs
See VLANs
reset command 72-3
resetting an interface to default configuration 8-40
resetting a switch to defaults 3-32
Resilient Ethernet ProtocolLSee REP
responder, IP SLAs
described 67-4
enabling 67-7
response time, measuring with IP SLAs 67-4
restricting access
NTP services 4-8
RADIUS 45-95
TACACS+ 3-15
retransmission number
setting in 802.1X authentication 45-86
retransmission time
changing in 802.1X authentication 45-85
RFC
1157, SNMPv1 61-2
1305, NTP 4-2
1757, RMON 67-2
1901, SNMPv2C 61-2
1902 to 1907, SNMPv2 61-2
2273-2275, SNMPv3 61-2
RFC 5176 Compliance 45-98
RIP
description 1-19
for IPv6 53-5
RIP, introduction 1-19
RMON
default configuration 67-3
displaying status 67-6
enabling alarms and events 67-3
groups supported 67-2
overview 67-1
ROM monitor
boot process and 3-26
CLI 2-7
commands 72-2 to 72-3
debug commands 72-5
entering 72-1
exiting 72-6
overview 72-1
root bridge
configuring 21-9
selecting in MST 21-22
root guard
and MST 21-23
enabling 24-2
overview 24-2
routed packets
ACLs 52-26
route-map (IP) command 39-6, 39-9
route maps
defining 39-6, 39-9
PBR 39-2
router ACLs
description 1-41, 52-3

using with VLAN maps 52-25
router ACLs, using PACL with VLAN maps 52-32
route targets
VPN 40-3
Routing Information Protocol
See RIP
RPF
See Unicast RPF
RSPAN
configuration guidelines 56-16
destination ports 56-5
IDS 56-2
monitored ports 56-4
monitoring ports 56-5
received traffic 56-3
sessions
creating 56-17
defined 56-3
limiting source traffic to specific VLANs 56-23
monitoring VLANs 56-21
removing source (monitored) ports 56-20
specifying monitored ports 56-17
source ports 56-4
transmitted traffic 56-4
VLAN-based 56-5
RSTP
compatibility 21-23
description 21-22
port roles 21-24
port states 21-24

S

S/M, 224/4 36-13
SAID
See 802.10 SAID
SAP
defined 44-9
negotiation 44-9
support 44-1
scheduling 41-8
scheduling, IP SLAs operations 67-5
secondary edge port, REP 23-4
secondary root switch 21-12
secondary VLANs 43-2
associating with primary 43-16
permitting routing 43-23
security
configuring 49-1
Security Association Identifier
See 802.10 SAID
Security Exchange Protocol
See SXP
Security Exchange Protocol
See SAP
selecting a power management mode 13-10
selecting X2/TwinGig Convertor Mode 8-14
sequence numbers in log messages 59-7
server IDs
description 66-23
service policy, configure class-level queue-limit 41-31, 41-65
service-policy input command 32-2
service-provider networks
and customer VLANs 28-2
session keys, MKA 44-2
set default interface command 39-7, 39-8, 39-9, 39-10
set interface command 39-7, 39-9
set ip default next-hop command 39-7, 39-9
set ip next-hop command 39-6, 39-7, 39-9, 39-12
set-request operation 61-4
severity levels, defining in system messages 59-8
shaping, QoS on Sup 6-E 41-25, 41-59
sharing(bandwidth), QoS on Sup 6-E 41-27, 41-61
Shell functions
See Auto SmartPorts macros
See Auto Smartports macros
Shell triggers

See Auto SmartPorts macros
See Auto Smartports macros
show adjacency command 34-9
show boot command 3-32
show catalyst4000 chassis-mac-address command 21-3
show cdp command 29-2, 29-3
show cdp entry command 29-4
show cdp interface command 29-3
show cdp neighbors command 29-4
show cdp traffic command 29-4
show ciscoview package command 4-48
show ciscoview version command 4-48
show cluster members command 15-13
show configuration command 8-23
show debugging command 29-4
show environment command 13-2
show history command 2-4
show interfaces command 8-28, 8-29, 8-36, 8-38
show interfaces status command 9-2
show ip cef command 34-8
show ip eigrp interfaces command 33-19
show ip eigrp neighbors command 33-19
show ip eigrp topology command 33-19
show ip eigrp traffic command 33-19
show ip interface command 36-23
show ip local policy command 39-11
show ip mroute command 36-23
show ip pim interface command 36-23
show l2protocol command 28-18
show lldp traffic command 30-15
show mac-address-table address command 9-3
show mac-address-table interface command 9-3
show mls entry command 34-8
show module command 9-1, 21-6
show PoE consumed 14-8
show power inline command 14-6
show power supplies command 13-13
show protocols command 8-36
show running-config command
adding description for an interface 8-23
checking your settings 3-9
displaying ACLs 52-19, 52-21, 52-30, 52-31
show startup-config command 3-10
show users command 9-6
show version command 3-29
shutdown, command 8-37
shutdown threshold for Layer 2 protocol packets 28-16
shutting down
interfaces 8-37
Simple Network Management Protocol
See SNMP
single-host mode 45-7
single spanning tree
See SST
single static RP, configuring 36-20
slot numbers, description 8-2
Slow timer, configuring BFD 38-16
smart call home 66-1
description 66-2
destination profile (note) 66-5
registration requirements 66-3
service contract requirements 66-3
Transport Gateway (TG) aggregation point 66-2
SMARTnet
smart call home registration 66-3
Smartports macros
applying global parameter values 19-8, 19-15
applying macros 19-8
applying parameter values 19-9
configuration guidelines 19-6, 19-14
configuring 19-2
creating 19-8
default configuration 19-4, 19-13
defined 1-10, 19-1
displaying 19-13
tracing 19-7, 19-14
SNMP
accessing MIB variables with 61-4

agent
described 61-4
disabling 61-7
and IP SLAs 67-2
authentication level 61-10
community strings
configuring 61-7
overview 61-4
configuration examples 61-15
configuration guidelines 61-6
default configuration 61-5
enabling 71-4, 71-5
engine ID 61-6
groups 61-6, 61-9
host 61-6
informs
and trap keyword 61-11
described 61-5
differences from traps 61-5
enabling 61-14
limiting access by TFTP servers 61-15
limiting system log messages to NMS 59-9
manager functions 61-3
notifications 61-5
overview 61-1, 61-4
status, displaying 61-16
system contact and location 61-14
trap manager, configuring 61-13
traps
described 61-3, 61-5
differences from informs 61-5
enabling 61-11
enabling MAC address notification 4-31
enabling MAC move notification 4-33
enabling MAC threshold notification 4-35
overview 61-1, 61-4
types of 61-11
users 61-6, 61-9
versions supported 61-2
SNMP commands 71-4
SNMP traps
REP 23-14
SNMPv1 61-2
SNMPv2C 61-2
SNMPv3 61-2
software
upgrading 10-13, 11-12
software configuration register 3-26
software QoS, on Sup 6-E 41-40, 41-74
software switching
description 34-5
interfaces 34-6
key data structures used 36-8
source IDs
call home event format 66-22
SPAN
and ACLs 56-5
configuration guidelines 56-7
configuring 56-7 to 56-10
destination ports 56-5
IDS 56-2
monitored port, defined 56-4
monitoring port, defined 56-5
received traffic 56-3
sessions
defined 56-3
source ports 56-4
transmitted traffic 56-4
VLAN-based 56-5
SPAN and RSPAN
concepts and terminology 56-3
default configuration 56-6
displaying status 56-24
overview 56-1
session limits 56-6
SPAN enhancements
access list filtering 56-13
configuration example 56-15

CPU port sniffing 56-10
encapsulation configuration 56-12
ingress packets 56-12
packet type filtering 56-14
spanning-tree backbonefast command 24-16
spanning-tree cost command 21-15
spanning-tree guard root command 24-2
spanning-tree portfast bpdu-guard command 24-8
spanning-tree portfast command 24-7
spanning-tree port-priority command 21-13
spanning-tree uplinkfast command 24-12
spanning-tree vlan
command 21-9
command example 21-9
spanning-tree vlan command 21-8
spanning-tree vlan cost command 21-16
spanning-tree vlan forward-time command 21-19
spanning-tree vlan hello-time command 21-18
spanning-tree vlan max-age command 21-18
spanning-tree vlan port-priority command 21-13
spanning-tree vlan priority command 21-17
spanning-tree vlan root primary command 21-10
spanning-tree vlan root secondary command 21-12
speed
configuring interface 8-20
speed command 8-21
SSO
configuring 12-10
SSO operation 12-4
SST
description 21-22
interoperability 21-24
static ACL, removing the requirement 52-28
static addresses
See addresses
static routes
configuring 3-11
verifying 3-12
statistics
802.1X 47-14
displaying 802.1X 45-125
displaying PIM 36-27
LLDP 30-14
LLDP-MED 30-14
MKA 44-4
SNMP input and output 61-16
sticky learning
configuration file 48-6
defined 48-5
disabling 48-6
enabling 48-5
saving addresses 48-6
sticky MAC addresses
configuring 48-7
defined 48-4
storing captured packets to a .pcap file, Wireshark 57-8
Storm Control
displaying 55-6
enabling Broadcast 55-3
enabling Multicast 55-4
hardware-based, implementing 55-2
overview 55-1
software-based, implementing 55-2
STP
and REP 23-6
bridge ID 21-2
configuring 21-7 to 21-20
creating topology 21-5
defaults 21-7
disabling 21-20
enabling 21-8
enabling extended system ID 21-9
enabling Per-VLAN Rapid Spanning Tree 21-20
EtherChannel guard
disabling 24-6
forward-delay time 21-19
hello time 21-17
Layer 2 protocol tunneling 28-13

maximum aging time 21-18
overview 21-1, 21-3
per-VLAN rapid spanning tree 21-6
port cost 21-15
port priority 21-13
root bridge 21-9
stratum, NTP 4-2
stub routing (EIGRP)
benefits 33-17
configuration tasks 33-18
configuring 33-14
overview 33-13, 33-14
restrictions 33-17
verifying 33-18
subdomains, private VLAN 43-2
summer time 4-13
supervisor engine
accessing the redundant 10-14, 11-14
configuring 3-8 to 3-13
copying files to standby 10-14, 11-14
default configuration 3-1
default gateways 3-11
environmental monitoring 13-1
redundancy 12-1
ROM monitor 3-26
startup configuration 3-25
static routes 3-11
synchronizing configurations 10-11, 11-10
Supervisor Engine 7L-E, selecting the uplink port 8-18
Supervisor Engine II-TS
insufficient inline power handling 13-22, 14-12
Smartports macros
See also Auto Smartports macros
SVI Autostate Exclude
understanding 33-3
SVI Autostate exclude
configuring 33-7
S-VLAN 1-2, 28-7
switch 53-2
switch access with RADIUS, controlling 45-95
switched packets
and ACLs 52-25
Switched Port Analyzer
See SPAN
switchport
show interfaces 8-28, 8-29, 8-38
switchport access vlan command 18-5, 18-7
switchport block multicast command 54-2
switchport block unicast command 54-2
switchport mode access command 18-7
switchport mode dot1q-tunnel command 28-6
switchport mode dynamic command 18-5
switchport mode trunk command 18-5
switch ports
See access ports
switchport trunk allowed vlan command 18-5
switchport trunk encapsulation command 18-5
switchport trunk native vlan command 18-5
switchport trunk pruning vlan command 18-6
switch-to-RADIUS server communication
configuring 45-32
sysret command 72-5
system
reviewing configuration 3-10
settings at startup 3-27
system alarms
overview 13-6
system and network statistics, displaying 36-23
system capabilities TLV 30-2
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 30-2
system images
loading from Flash memory 3-30
modifying boot field 3-27
specifying 3-30
system message logging
default configuration 59-3
defining error message severity levels 59-8
disabling 59-4
displaying the configuration 59-12
enabling 59-4
facility keywords, described 59-12
level keywords, described 59-9
limiting messages 59-9
message format 59-2
overview 59-1
sequence numbers, enabling and disabling 59-7
setting the display destination device 59-5
synchronizing log messages 59-6
timestamps, enabling and disabling 59-7
UNIX syslog servers
configuring the daemon 59-10
configuring the logging facility 59-11
facilities supported 59-12
system MTU
802.1Q tunneling 28-5
maximums 28-5
system name
manual configuration 4-22
See also DNS
system name TLV 30-2
system prompt, default setting 4-21

T

TACACS+ 49-1
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 28-3
Layer 2 protocol 28-13
TCAM programming and ACLs 52-7
for Sup II-Plust thru V-10GE 52-6
TCAM programming and ACLs for Sup 6-E 52-10
TDR
checking cable connectivity 9-3
enabling and disabling test 9-3
guidelines 9-3
Telnet
accessing CLI 2-2
disconnecting user sessions 9-7
executing 9-5
monitoring user sessions 9-6
telnet command 9-6
templates, Ethernet OAM 64-45
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 61-15
TFTP download
See also console download
threshold monitoring, IP SLAs 67-6
time

See NTP and system clock
Time Domain Reflectometer
See TDR
time exceeded messages 9-9
timer
See login timer
timestamps in log messages 59-7
time zones 4-12
TLV
host presence detection 45-8
TLVs
defined 1-7, 30-2
LLDP-MED 30-2
Token Ring
media not supported (note) 16-5, 16-10
Topology change notification processing
MLD Snooping
Topology change notification processing 27-4
TOS
description 41-4
trace command 9-9
traceroute
See IP traceroute
See Layer 2 Traceroute
traceroute mac command 9-11
traceroute mac ip command 9-11
tracked lists
configuring 58-3
types 58-3
tracked objects
by Boolean expression 58-4
by threshold percentage 58-6
by threshold weight 58-5
tracking interface line-protocol state 58-2
tracking IP routing state 58-2
tracking objects 58-1
tracking process 58-1
track state, tracking IP SLAs 58-9
traffic
blocking flooded 54-2
traffic control
using ACLs (figure) 52-4
using VLAN maps (figure) 52-5
traffic marking procedure flowchart 41-21, 41-55
traffic shaping 41-9
translational bridge numbers (defaults) 16-5
traps
configuring MAC address notification 4-31
configuring MAC move notification 4-33
configuring MAC threshold notification 4-35
configuring managers 61-11
defined 61-3
enabling 4-31, 4-33, 4-35, 61-11
notification types 61-11
overview 61-1, 61-4
troubleshooting
with CiscoWorks 61-4
with system message logging 59-1
with traceroute 9-8
troubleshooting high CPU due to ACLs 52-6
trunk failover
See link-state tracking
trunk ports
configure port security 48-17
configuring PVLAN 43-19 to 43-21
trunks
802.1Q restrictions 18-4
configuring 18-5
configuring access VLANs 18-5
configuring allowed VLANs 18-5
default interface configuration 18-5
enabling to non-DTP device 18-3
specifying native VLAN 18-5
understanding 18-3
trustpoint 66-3
tunneling
defined 28-1
tunnel ports

802.1Q, configuring 28-6
described 28-2
incompatibilities with other features 28-5
TwinGig Convertors
limitations on using 8-14
port numbering 8-13
selecting X2/TwinGig Convertor mode 8-14
type length value
See TLV
type of service
See TOS

U

UDLD
configuring probe message interval per-interface 31-8
default configuration 31-4
disabling on fiber-optic interfaces 31-7
disabling on non-fiber-optic interfaces 31-7
displaying link status 31-9
enabling globally 31-5
enabling per-interface 31-6
modes of operation 31-3
resetting disabled LAN interfaces 31-8
use case 31-2
UDLD, overview 31-1
UDP jitter, configuring 67-9
UDP jitter operation, IP SLAs 67-8
unauthorized ports with 802.1X 45-5
unicast
See IP unicast
unicast flood blocking
configuring 54-1
unicast MAC address filtering
and adding static addresses 4-38
and broadcast MAC addresses 4-37
and CPU packets 4-37
and multicast addresses 4-37
and router MAC addresses 4-37
configuration guidelines 4-37
described 4-37
unicast MAC address filtering, configuring
ACLs
configuring unicast MAC address filtering 52-13
Unicast RPF (Unicast Reverse Path Forwarding)
applying 35-5
BGP attributes
caution 35-4
CEF
requirement 35-2
tables 35-7
configuring 35-9
(examples) ?? to 35-12
BOOTP 35-8
DHCP 35-8
enterprise network (figure) 35-6
prerequisites 35-9
routing table requirements 35-7
tasks 35-9
verifying 35-10
deploying 35-5
description 1-22, 35-1
disabling 35-11
enterprise network (figure) 35-6
FIB 35-2
implementing 35-4
packets, dropping (figure) 35-4
prerequisites 35-9
restrictions
basic 35-8
routing asymmetry 35-7
routing asymmetry (figure) 35-8
routing table requirements 35-7
security policy
applying 35-5
attacks, mitigating 35-5
deploying 35-5

tunneling 35-5
source addresses, validating 35-3
(figure) 35-3, 35-4
failure 35-3
traffic filtering 35-5
tunneling 35-5
validation
failure 35-3, 35-4
packets, dropping 35-3
source addresses 35-3
verifying 35-10
unicast traffic
blocking 54-2
Unidirectional Controlled Port, configuring 802.1X 45-66
unidirectional ethernet
enabling 32-2
example of setting 32-2
overview 32-1
UniDirectional Link Detection Protocol
See UDLD
Universal PoE, configuring 14-16
UNIX syslog servers
daemon configuration 59-10
facilities supported 59-12
message logging configuration 59-11
UplinkFast
and MST 21-23
enabling 24-15
MST and 21-23
overview 24-11
uplink forwarding
quad-supervisor 5-6
uplink mode, selecting on supervisor engine 6-E 8-16
uplink port, selecting on a supervisor engine 7L-E 8-18
usage examples, Wireshark 57-18
user-defined event triggers
configuring, 802.1X-based 20-8
configuring, MAC address-based 20-9
User-defined triggers and built-in macros, configuring mapping 20-9
user EXEC mode 2-5
user sessions
disconnecting 9-7
monitoring 9-6

V

VACLs
Layer 4 port operations 52-10
virtual configuration register 72-3
virtual LANs
See VLANs
virtual ports, MKA 44-3
Virtual Router Redundancy Protocol, introduction 1-22
Virtual Switch System(VSS), displaying EtherChannel to 25-16
VLAN ACLs
See VLAN maps
VLAN blocking, REP 23-13
vlan command 16-6
vlan dot1q tag native command 28-4
VLAN ID
service provider 28-9
VLAN ID, discovering 4-44
VLAN ID translation
See VLAN mapping
VLAN load balancing
REP 23-4
VLAN load balancing, triggering 23-6
VLAN load balancing on flex links 22-2
configuration guidelines 22-6
VLAN Management Policy Server
See VMPS
VLAN mapping
1-to-1 28-8
1-to-1, configuring 28-11
configuration guidelines 28-10

configuring 28-11
configuring on a trunk port 28-11
default 28-9
described 1-2, 28-7
selective QinQ 28-8
selective Q-in-Q, configuring 28-12
traditional QinQ 28-8
traditional Q-in-Q, configuring 28-12
types of 28-8
VLAN maps
applying to a VLAN 52-21
configuration example 52-22
configuration guidelines 52-18
configuring 52-17
creating and deleting entries 52-19
defined 1-41
denying access example 52-23
denying packets 52-19
displaying 52-24
order of entries 52-18
permitting packets 52-19
router ACLs and 52-25
using (figure) 52-5
using in your network 52-22
VLAN maps, PACL and Router ACLs 52-32
VLANs
allowed on trunk 18-5
configuration guidelines 16-3
configuring 16-5
configuring as Layer 3 interfaces 33-7
customer numbering in service-provider networks 28-3
default configuration 16-4
description 1-11
extended range 16-3
IDs (default) 16-5
interface assignment 16-7
limiting source traffic with RSPAN 56-23
monitoring with RSPAN 56-21
name (default) 16-5
normal range 16-3
overview 16-1
reserved range 16-3
See also PVLANs
VLAN Trunking Protocol
See VTP
VLAN trunks
overview 18-3
VLAN User Distribution, configuring 802.1X 45-68
VMPS
configuration file example 16-32
configuring dynamic access ports on client 16-25
configuring retry interval 16-27
database configuration file 16-32
dynamic port membership
example 16-29
reconfirming 16-26
reconfirming assignments 16-26
reconfirming membership interval 16-26
server overview 16-21
VMPS client
administering and monitoring 16-27
configure switch
configure reconfirmation interval 16-26
dynamic ports 16-25
entering IP VMPS address 16-24
reconfirmation interval 16-27
reconfirm VLAM membership 16-26
default configuration 16-24
dynamic VLAN membership overview 16-23
troubleshooting dynamic port VLAN membership 16-28
VMPS server
fall-back VLAN 16-22
illegal VMPS client requests 16-23
overview 16-21
security modes
multiple 16-22

open 16-21
secure 16-22
voice aware 802.1x security
port-based authentication
configuring 45-74
described 45-22, 45-73
voice interfaces
configuring 42-1
Voice over IP
configuring 42-1
voice ports
configuring VVID 42-3
voice traffic 14-2, 42-5
voice VLAN
IP phone data traffic, described 42-2
IP phone voice traffic, described 42-2
Voice VLAN, configure 802.1X 45-72
voice VLAN ports
using 802.1X 45-22
VPN
configuring routing in 40-8
forwarding 40-3
routes 40-2
routing and forwarding table
See VRF
VRF
defining 40-3
tables 40-1
VRF-aware services
ARP 40-6, 40-15, 40-17
configuring 40-6, 40-15
ftp 40-16
ping 40-15
tftp 40-16
traceroute 40-16
uRPF 40-16
VRF-lite
description 1-22
VSS
dual-active detection
displaying 5-51
Enhanced PAgP, advantages 5-23
enhanced PAgP, configuring 5-49
Enhanced PAgP, description 5-23
fast-hello, configuring 5-50
VTP
client, configuring 16-16
configuration guidelines 16-12
default configuration 16-13
disabling 16-16
Layer 2 protocol tunneling 28-14
monitoring 16-19
overview 16-8
pruning
configuring 16-15
See also VTP version 2
server, configuring 16-16
statistics 16-19
transparent mode, configuring 16-16
version 2
enabling 16-15
VTP advertisements
description 16-9
VTP domains
description 16-8
VTP modes 16-9
VTP pruning
overview 16-11
VTP versions 2 and 3
overview 16-9
See also VTP
VTY and Network Assistant 15-12
VVID (voice VLAN ID)
and 802.1X authentication 45-22
configuring 42-3

W

WCCP
- configuration examples 70-10
- configuring on a router 70-2, 70-11
- features 70-4
- restrictions 70-5
- service groups 70-6

web-based authentication
- authentication proxy web pages 47-4
- description 1-43, 45-14, 47-1

web-based authentication, interactions with other features 47-4

Web Cache Communication Protocol
- See WCCP 70-1

web caches
- See cache engines

web cache services
- description 70-4

web caching
- See web cache services
- See also WCCP

web scaling 70-1

weight thresholds in tracked lists 58-5

Wireshark
- activating and deactivating, capture points, conceptual 57-9
- attachment points 57-6
- capture filter 57-7
- capture points 57-6
- core system filter 57-6
- decoding and displaying packets 57-9
- display filter 57-7
- feature interactions 57-10
- filters 57-6
- storing captured packets to a .pcap filter 57-8
- usage examples 57-18

Wireshark, about 57-5

Wireshark, activating and deactivating a capture point 57-13

Wireshark, defining/modifying/deleting a capture point 57-12

Wireshark, displaying information 57-14

WS-X46490-CSFP-E, support on a 10-slot chassis 8-17

Y

Y.1731
- default configuration 64-29
- described 64-27
- ETH-AIS
  - Ethernet Alarm Signal function (ETH-AIS) 64-28
- ETH-RDI 64-28
- multicast Ethernet loopback 64-31
- multicast ETH-LB 64-29
- terminology 64-27