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 14-21

1400 W DC SP Triple Input power supply
- special considerations 14-22

802.10 SAID (default) 17-5

802.1AE
- standard 45-2

802.1Q
- trunks 22-6
- tunneling
  - compatibility with other features 29-5
  - defaults 29-3
  - described 29-2
- tunnel ports with other features 29-6

802.1Q VLANs
- trunk restrictions 19-4

802.1s
- See MST

802.1w
- See MST

802.1X
- See port-based authentication

802.1X authentication
- Authentication Failed VLAN assignment 46-17
- for Critical Authentication 46-14
- for guest VLANs 46-11
- for MAC Authentication Bypass 46-12
- for Unidirectional Controlled Port 46-15
- VLAN User Distribution 46-16
- web-based authentication 46-14
- with port security 46-19
- with VLAN assignment 46-10
- with voice VLAN ports 46-22

802.1X Host Mode 46-6
- multiauthentication mode 46-8
- multidomain authentication mode 46-7
- single-host 46-7

802.1x-REV 45-2

802.3ad
- See LACP

9000W AC, displaying OBFL 14-4

A

AAA 50-1

AAA (authentication, authorization, and accounting). See also port-based authentication. 48-2

abbreviating commands 2-5

about Wireshark 58-5

access control entries
- See ACEs

access control entries and lists 50-1

access-group mode, configuring on Layer 2 interface 53-31

access-group mode, using PACL with 53-30

access list filtering, SPAN enhancement 57-13

access lists
- using with WCCP 71-8

access ports

and Layer 2 protocol tunneling 29-15
configure port security 49-7, 49-22
configuring 19-7
access VLANs 19-5
accounting
with RADIUS 46-111
with TACACS+ 3-16, 3-21
ACEs
ACLs 53-2
IP 1-41, 53-2
Layer 4 operation restrictions 53-10
ACEs and ACLs 50-1
ACL assignments, port-based authentication 46-20
ACL assignments and redirect URLs, configure 46-38
ACL configuration, displaying a Layer 2 interface 53-32
ACLs
ACEs 53-2
and SPAN 57-5
and TCAM programming for Sup 6-E 53-10
and TCAM programming for Sup II-Plus thru V-10GE 53-6
applying IPv6 ACLs to a Layer 3 interface 53-17
applying on routed packets 53-26
applying on switched packets 53-25
compatibility on the same switch 53-3
configuring with VLAN maps 53-25
CPU impact 53-12
downloadable 48-7
hardware and software support 53-6
IP, matching criteria for port ACLs 53-4
MAC extended 53-14
matching criteria for router ACLs 53-3
port
and voice VLAN 53-4
defined 53-3
processing 53-12
selecting mode of capturing control packets 53-7
troubleshooting high CPU 53-6
types supported 53-3
understanding 53-2
VLAN maps 53-5
ACLs, applying to a Layer 2 interface 53-31
ACLs and VLAN maps, examples 53-19
acronyms, list of 1-1
action drivers, marking 42-21, 42-55
activating and deactivating a capture point, Wireshark 58-13
activating and deactivating Wiresharkcapture points, conceptual, Wireshark 58-9
active queue management 42-9
active queue management via DBL, QoS on Sup 6-E 42-34, 42-68
active traffic monitoring, IP SLAs 68-1
adding members to a community 16-9
addresses
displaying the MAC table 4-44
dynamic
changing the aging time 4-30
defined 4-28
learning 4-29
removing 4-31
IPv6 54-2
MAC, discovering 4-44
See MAC addresses
static
adding and removing 4-36
defined 4-28
address resolution 4-44
adjacency tables
description 35-2
displaying statistics 35-9
administrative VLAN
REP, configuring 24-9
administrative VLAN, REP 24-8
advertisements
LLDP 1-7, 31-2
advertisements, VTP
See VTP advertisements
aggregation switch, enabling DHCP snooping 52-9

aging time
MAC address table 4-30
All Auth manager sessions, displaying summary 46-126
All Auth manager sessions on the switch authorized for a specified authentication method 46-126
ANCP client
enabling and configuring 38-2
guidelines and restrictions 38-5
identify a port with DHCP option 82 38-4
identify a port with protocol 38-2
overview 38-1
ANCP protocol
identifying a port with 38-2
applying IPv6 ACLs to a Layer 3 interface 53-17
AQM via DBL, QoS on Sup 6-E 42-34, 42-68
archiving crashfiles information 2-8
ARP
defined 4-44
table
address resolution 4-44
managing 4-44
asymmetrical links, and 802.1Q tunneling 29-3
attachment points, Wireshark 58-6
attributes, RADIUS
vendor-proprietary 46-114
vendor-specific 46-112
authentication
NTP associations 4-4
RADIUS
key 46-104
login 46-106
See also port-based authentication
TACACS+
defined 3-16
key 3-18
login 3-19
Authentication, Authorization, and Accounting (AAA) 50-1
Authentication Failed, configuring 80.1X 46-70
Authentication methods registered with the Auth manager, determining 46-125
authentication open comand 46-8
authentication proxy web pages 48-4
authentication server
defined 46-3
RADIUS server 46-3
Auth manager session for an interface, verifying 46-126
Auth manager summary, displaying 46-126
authoritative time source, described 4-2
authorization
with RADIUS 46-110
with TACACS+ 3-16, 3-21
authorized and unauthorized ports 46-5
authorized ports with 802.1X 46-5
autoconfiguration 3-2
automatic discovery
considerations 16-7
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 21-6
Auto SmartPorts macros
built-in macros 21-5
configuration guidelines 21-5
default configuration 21-4
defined 21-1
displaying 21-13
enabling 21-4
IOS shell 21-2, 21-10
Auto Smartports macros
defined 1-2
Auto SmartPorts user-defined macros
configuring 21-10
auto-sync command 11-8, 12-7

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) 25-3
and MST 22-23
configuring 25-15
link failure (figure) 25-14, 25-15
not supported MST 22-23
understanding 25-13
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 73-3
BFD
and hardware support 39-7
configuration example
BFD in a BGP network 39-25
BFD in an EIGRP network with echo mode enabled by default 39-17
BFD in an OSPF network 39-22
support for static routing 39-27
configuring
Echo mode 39-15
session parameters on the interface 39-8
Slow timer 39-16
support for BGP 39-9
support for dynamic routing protocols 39-9
support for EIGRP 39-10
support for OSPF 39-11
support for static routing 39-13
disabling echo mode without asymmetry 39-16
monitoring and troubleshooting 39-17
neighbor relationships 39-3
operation 39-3
prerequisites 39-2
restrictions 39-2
b flash command 73-3
BGP 1-17
routing session with multi-VRF CE 41-9
blocking packets 55-1
blocking state (STP)
RSTP comparisons (table) 22-24
Boolean expressions in tracked lists 59-4
boot bootldr command 3-31
boot command 3-28
boot commands 73-3
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 22-27
BPDU Guard
and MST 22-23
configuring 25-15
overview 25-8
BPDUs
and media speed 22-2
pseudobridges and 22-25
what they contain 22-3
bridge ID
See STP bridge ID
bridge priority (STP) 22-17

bridge protocol data units
See BPDUs
Broadcast Storm Control
disabling 56-5
enabling 56-3
Built-in macros and user-defined triggers, configuring
mapping 21-9

C

cache engine clusters 71-1
cache engines 71-1
cache farms
See cache engine clusters
Call Home
description 1-24, 67-2
message format options 67-2
messages
format options 67-2
call home 67-1
alert groups 67-6
configuring e-mail options 67-9
contact information 67-4
default settings 67-18
destination profiles 67-5
displaying information 67-14
mail-server priority 67-10
pattern matching 67-9
periodic notification 67-8
rate limit messages 67-9
severity threshold 67-8
smart call home feature 67-2
SMTP server 67-9
testing communications 67-10
call home alert groups
configuring 67-6
description 67-6
subscribing 67-7
call home contacts
assigning information 67-4
call home destination profiles
attributes 67-5
configuring 67-5
description 67-5
displaying 67-16
call home notifications
full-txt format for syslog 67-25
XML format for syslog 67-28
candidates
automatic discovery 16-7
candidate switch, cluster
defined 16-12
capture filter, Wireshark 58-7
capture points, Wireshark 58-6
Capturing control packets
selecting mode 53-7
cautions
Unicast RPF
BGP optional attributes 36-4
cautions for passwords
encrypting 3-22
CDP
automatic discovery in communities 16-7
configuration 30-2
defined with LLDP 31-1
displaying configuration 30-3
enabling on interfaces 30-3
host presence detection 46-8
Layer 2 protocol tunneling 29-13
maintaining 30-3
monitoring 30-3
overview 1-3, 30-1
cdp enable command 30-3
CEF
adjacency tables 35-2
and NSF with SSO 13-5
configuring load balancing 35-7
displaying statistics 35-8

enabling 35-6, 70-2
hardware switching 35-4
load balancing 35-6
overview 35-1
software switching 35-4
certificate authority (CA) 67-3
CFM
and Ethernet OAM, configuring 65-51
and Ethernet OAM interaction 65-51
clearing 65-31
configuration guidelines 65-7, 66-4
configuring crosscheck for VLANs 65-11
configuring fault alarms 65-16
configuring port MEP 65-14
configuring static remote MEP 65-13, 65-16, 65-18
crosscheck 65-5
defined 65-2
EtherChannel support 65-7, 66-4
fault alarms
configuring 65-16
IP SLAs support for 65-6
IP SLAs with endpoint discovers 65-21
maintenance domain 65-2
manually configuring IP SLAs ping or jitter 65-19
measuring network performance 65-6
monitoring 65-32, 65-33
port MEP, configuring 65-14
remote MEPs 65-5
static RMEP, configuring 65-13, 65-16, 65-18
static RMEP check 65-5
Y.1731
described 65-27
CGMP
overview 27-2
Change of Authorization, RADIUS 46-97
channel-group group command 5-46, 26-8, 26-10
Cisco 7600 series Internet router
enabling SNMP 72-4, 72-5
Cisco Discovery Protocol
See CDP
Cisco Express Forwarding
See CEF
Cisco Group Management Protocol
See CGMP
Cisco IOS IP SLAs 68-2
Cisco IOS NSF-aware
support 13-2
Cisco IOS NSF-capable support 13-2
Cisco IP Phones
configuring 43-3
sound quality 43-1
Cisco TrustSec
credentials 45-10
switch-to-switch security
802.1x mode 45-11
configuration example 45-14
manual mode 45-12
Cisco TrustSec Network Device Admission Control
See NDAC
CiscoWorks 2000 62-4
CIST
description 22-22
civic location 31-3
class level, configure in a service policy 42-31, 42-65
class of service
See CoS
clear cdp counters command 30-4
clear cdp table command 30-3
clear counters command 8-36
clearing
Ethernet CFM 65-31
IP multicast table entries 37-28
clear ip eigrp neighbors command 34-19
CLI
accessing 2-2
backing out one level 2-5
getting commands 2-5
history substitution 2-4

managing clusters 16-13
modes 2-5
monitoring environments 57-1
ROM monitor 2-7
software basics 2-4
client processes, tracking 59-1
clients
in 802.1X authentication 46-3
clock
See system clock
clustering switches
command switch characteristics
and VTY 16-12
convert to a community 16-10
managing
through CLI 16-13
overview 16-2
planning considerations
CLI 16-13
passwords 16-8
CoA Request Commands 46-100
command-line processing 2-3
command modes 2-5
commands
b 73-3
b flash 73-3
boot 73-3
confreg 73-3
dev 73-3
dir device 73-3
frame 73-5
i 73-3
listing 2-5
meminfo 73-5
reset 73-3
ROM monitor 73-2 to 73-3
ROM monitor debugging 73-5
SNMP 72-4
sysret 73-5
command switch, cluster
requirements 16-11
common and internal spanning tree
See CIST
common spanning tree
See CST
community of switches
access modes in Network Assistant 16-9
adding devices 16-9
communication protocols 16-8
community name 16-8
configuration information 16-9
converting from a cluster 16-10
host name 16-8
passwords 16-8
community ports 44-3
community strings
configuring 62-7
overview 62-4
community VLANs 44-2, 44-3
configure as a PVLAN 44-15
compiling MIBs 72-4
config-register command 3-29
config terminal command 3-9
configurable leave timer,IGMP 27-4
configuration examples
SNMP 62-15
configuration files
limiting TFTP server access 62-15
obtaining with DHCP 3-6
saving 3-10
system contact and location information 62-14
configuration guidelines
CFM 65-7, 66-4
Ethernet OAM 65-35
REP 24-7
SNMP 62-6
VLAN mapping 29-10
configuration register

boot fields
listing value 3-29
modifying 3-28
changing from ROM monitor 73-3
changing settings 3-28 to 3-29
configuring 3-26
settings at startup 3-27
configure class-level queue-limit in a service policy 42-31, 42-65
configure terminal command 3-29, 8-2
configuring access-group mode on Layer 2 interface 53-31
configuring flow control 8-23
configuring interface link and trunk status envents 8-37
configuring named IPv6 ACLs 53-16
configuring named MAC extended ACLs 53-14, 53-15
configuring unicast MAC address filtering 53-13
configuring VLAN maps 53-17
confreg command 73-3
Connectivity Fault Management
See CFM
console configuration mode 2-5
console download 73-4 to 73-5
console port
disconnecting user sessions 9-7
monitoring user sessions 9-6
contact information
assigning for call home 67-4
controlling switch access with RADIUS 46-95
Control Plane Policing
and Layer 2 Control packet QoS, configuration example 50-14
configuration guidelines and restrictions 50-8
configuring for control plane traffic 50-4
configuring for data plane and management plan traffic 50-5
defaults 50-4
general guidelines 50-3
monitoring 50-9
understanding 50-2
control protocol, IP SLAs 68-4
convergence
REP 24-4
copy running-config startup-config command 3-10
copy system:running-config nvram:startup-config command 3-32
core system filter, Wireshark 58-6
CoS
definition 42-3
figure 42-2
overriding on Cisco IP Phones 43-5
priority 43-5
counters
clearing MFIB 37-28
clearing on interfaces 8-36
CPU, impact of ACL processing 53-12
CPU port sniffing 57-10
crashfiles information, archiving 2-8
Critical Authentication
configure with 802.1X 46-62
crosscheck, CFM 65-5, 65-11
CST
description 22-25
IST and 22-22
MST and 22-22
customer edge devices 41-2
C-VLAN 1-2, 29-7

D

database agent
configuration examples 52-15
enabling the DHCP Snooping 52-13
daylight saving time 4-13
debug commands, ROM monitor 73-5
decoding and displaying packets, Wireshark 58-9
default configuration
802.1X 46-27
banners 4-24

DNS 4-23
Ethernet OAM 65-35
IGMP filtering 27-30
IGMP snooping 28-5, 28-6
IP SLAs 68-6
IPv6 54-7
Layer 2 protocol tunneling 29-16
LLDP 31-5
MAC address table 4-30
MVR 27-23
NTP 4-4
private VLANs 44-12
RADIUS 46-103
REP 24-7
resetting the interface 8-40
RMON 69-3
SNMP 62-5
SPAN and RSPAN 57-6
system message logging 60-3
TACACS+ 3-18
VLAN mapping 29-9
Y.1731 65-29
default gateway
configuring 3-11
verifying configuration 3-11
default settings, erase commad 3-32
default web-based authentication configuration
802.1X 48-6
defining/modifying/deleting a capture point, Wireshark 58-12
denial-of-service attacks
IP address spoofing, mitigating 36-5
Unicast RPF, deploying 36-5
denying access to a server on another VLAN 53-23
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 73-3
device discovery protocol 31-1
device IDs
call home format 67-21, 67-22
device sensor
configuring 46-118
DHCP
configuring
rate limit for incoming packets 52-13
denial-of-service attacks, preventing 52-13
rate limiting of packets
configuring 52-13
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 38-4
overview 52-4
DHCP Snooping
enabling, and Option 82 52-10
DHCP snooping
accepting untrusted packets form edge switch 52-10
configuring 52-6
default configuration 52-7
displaying binding tables 52-19
displaying configuration 52-19
displaying information 52-18
enabling 52-7
enabling on private VLAN 52-12

enabling on the aggregation switch 52-9
enabling the database agent 52-13
message exchange process 52-4
monitoring 52-23
option 82 data insertion 52-4
overview 52-1
Snooping database agent 52-2
DHCP Snooping Database Agent
adding to the database (example) 52-18
enabling (example) 52-15
overview 52-2
reading from a TFTP file (example) 52-17
Diagnostics
online 70-1
Power-On-Self-Test
causes of failure 70-20
how it works 70-10
overview 70-10
Power-On-Self-Test for Supervisor Engine V-10GE 70-13
Differentiated Services Code Point values
See DSCP values
DiffServ architecture, QoS 42-2
Digital optical monitoring transceiver support 8-19
dir device command 73-3
disabled state
RSTP comparisons (table) 22-24
disabling
broadcast storm control 56-5
disabling multicast storm control 56-5
disconnect command 9-7
discovery, clusters
See automatic discovery
discovery, Ethernet OAM 65-34
display dection and removal events 15-7
display filter, Wireshark 58-7
displaying
Auth Manager sumary for an interface 46-126
MAB details 46-128
summary of all Auth manager sessions 46-126
summary of all Auth manager sessions on the switch authorized for a specified authentication method 46-126
displaying EtherChannel to a Virtual Switch System 26-16
displaying storm control 56-6
displaying Wireshark information 58-14
display PoE consumed by a module 15-8
display PoE detection and removal events 15-7
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 29-2
Layer 2 protocol tunneling 29-15
downloading MIBs 72-3, 72-4
drop threshold for Layer 2 protocol packets 29-16
DSCP values
definition 42-4
IP precedence 42-2
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 51-2
configuring
ACLs for non-DHCP environments 51-11
in DHCP environments 51-5
log buffer 51-14

rate limit for incoming ARP packets 51-16
denial-of-service attacks, preventing 51-16
interface trust state, security coverage 51-3
log buffer
configuring 51-14
logging of dropped packets 51-4
overview 51-1
port channels, their behavior 51-5
priority of static bindings 51-4
purpose of 51-2
rate limiting of ARP packets 51-4
configuring 51-16
validation checks, performing 51-19
Dynamic Host Configuration Protocol snooping
See DHCP snooping
dynamic port VLAN membership
example 17-29
limit on hosts 17-28
reconfirming 17-26
troubleshooting 17-28

E

EAP frames
changing retransmission time 46-85
exchanging (figure) 46-4, 46-6, 46-13
request/identity 46-4
response/identity 46-4
setting retransmission number 46-86
EAPOL frames
802.1X authentication and 46-3
OTP authentication, example (figure) 46-4, 46-13
start 46-4
Echo mode,configuring BFD 39-15
edge ports
description 22-27
EGP
overview 1-17
EIGRP
configuration examples 34-19
monitoring and maintaining 34-19
EIGRP (Enhanced IGRP)
stub routing
benefits 34-17
configuration tasks 34-18
configuring 34-14
overview 34-14
restrictions 34-17
verifying 34-18
EIGRP (enhanced IGRP)
overview 1-17
eigrp stub command 34-18
EIGRP stub routing, configuring 34-13
ELIN location 31-3
e-mail addresses
assigning for call home 67-4
e-mail notifications
Call Home 1-24, 67-2
Embedded CiscoView
displaying information 4-48
installing and configuring 4-45
overview 4-45
emergency alarms on Sup Engine 6-E systems 14-5
enable command 3-9, 3-28
enable mode 2-5
enabling SNMP 72-4, 72-5
encryption keying 45-2
encryption keys, MKA 45-2
Enhanced Interior Gateway Routing Protocol
See EIGRP
enhanced object tracking
defined 59-1
IP routing state 59-2
line-protocol state 59-2
tracked lists 59-3
Enhanced PoE support on E-series 15-15
Enhanced PoE support on E-series,configuring Universal PoE 15-16

environmental monitoring
using CLI commands 14-1
EPM logging 46-129
errdisable recovery
configuring 15-14
EtherChannel
channel-group group command 5-46, 26-8, 26-10
configuration guidelines 5-30, 26-5
configuring 26-6 to 26-16
configuring (tasks) 5-30
configuring Layer 2 26-10
configuring Layer 3 26-7
DFC restriction, see CSCdt27074 in the Release Notes
displaying to a virtual switch system 26-16
interface port-channel command 26-7
lacp system-priority
command example 26-13
modes 26-3
overview 26-2
PAgP
Understanding 26-4
physical interface configuration 5-46, 26-7
port-channel interfaces 26-2
port-channel load-balance command 26-14
removing 26-15
removing interfaces 26-15
understanding 5-2
EtherChannel guard
disabling 25-6
enabling 25-6
overview 25-6
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 65-34
and CFM interaction 65-51
configuration guidelines 65-35
configuring with CFM 65-51
default configuration 65-35
discovery 65-34
enabling 65-36, 65-52
link monitoring 65-34, 65-38
messages 65-34
protocol
defined 65-33
monitoring 65-49
remote failure indications 65-34
remote loopback 65-34, 65-37
templates 65-45
Ethernet OAM protocol CFM notifications 65-51
Ethernet Remote Defect Indication (ETH-RDI) 65-28
event triggers, user-defined
configuring, 802.1X-based 21-8
configuring, MAC address-based 21-9
explicit host tracking
enabling 27-11
extended range VLANs
See VLANs
Extensible Authentication Protocol over LAN 46-2
Exterior Gateway Protocol
See EGP

F

Fa0 port
See Ethernet management port
Failure detection, using BFD 39-7
Fallback Authentication

configure with 802.1X 46-77
FastDrop
overview 37-11
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 32-8
default configuration 32-4
displaying link status 32-9
enabling globally 32-5
enabling on individual interface 32-7
enabling per-interface 32-6
modes of operation 32-3
resetting disabled LAN interfaces 32-8
use case 32-2
Fast UDLD, overview 32-1
feature interactions, Wireshark 58-10
FIB
description 35-2
See also MFIB
fiber-optics interfaces
disabling UDLD 32-7
Filter-ID ACL and Per-User ACL, configureport-based authentication
configure Per-User ACL and Filter-ID ACL 46-45
filtering
in a VLAN 53-18
non-IP traffic 53-14, 53-15
filters, Wireshark 58-6
flags 37-12
Flash memory
configuring router to boot from 3-31
loading system images from 3-30
security precautions 3-31
Flexible NetFlow
caveats 64-1, 64-7
defined 1-4, 64-1
Flex Links
configuration guidelines 23-6
configuring 23-6, 23-7
configuring preferred VLAN 23-9
configuring VLAN load balancing 23-8
monitoring 23-12
flooded traffic, blocking 55-2
flowchart, traffic marking procedure 42-21, 42-55
flow control, configuring 8-23
For 15-13
forward-delay time (STP)
configuring 22-19
forwarding information base
See FIB
frame command 73-5

G

gateway
See default gateway
get-bulk-request operation 62-3
get-next-request operation 62-3, 62-4
get-request operation 62-3, 62-4
get-response operation 62-3
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 46-57

H

hardware and software ACL support 53-6
hardware switching 35-5

hello time (STP)
configuring 22-17
high CPU due to ACLs, troubleshooting 53-6
history
CLI 2-4
history table, level and number of syslog messages 60-9
hop counts
configuring MST bridges 22-28
host
limit on dynamic port 17-28
host modes, MACsec 45-3
host ports
kinds of 44-4
host presence CDP message 46-8
Hot Standby Routing Protocol
See HSRP
HSRP
description 1-16
HSRP, introduction 1-16
hw-module module num power command 14-22

I

ICMP
enabling 9-12
ping 9-7
running IP traceroute 9-9
time exceeded messages 9-9
ICMP Echo operation
configuring 68-11
IP SLAs 68-11
i command 73-3
IDS
using with SPAN and RSPAN 57-2
IEEE 802.1ag 65-2
IEEE 802.1s
See MST
IEEE 802.1w
See MST
IEEE 802.3ad
See LACP
IGMP
configurable-leave timer 27-4
description 37-3
enabling 37-14
explicit host tracking 27-4
immediate-leave processing 27-3
leave processing, enabling 28-8
overview 27-2
report suppression
disabling 28-10
IGMP filtering
configuring 27-31
default configuration 27-30
described 27-30
monitoring 27-34
IGMP groups
setting the maximum number 27-33
IGMP Immediate Leave
configuration guidelines 27-9
IGMP profile
applying 27-32
configuration mode 27-31
configuring 27-31
IGMP Snooping
configure
leave timer 27-9
configuring
Learning Methods 27-7
static connection to a multicast router 27-8
configuring host statically 27-11
enabling
Immediate-Leave processing
explicit host tracking 27-11
suppressing multicast flooding 27-12
IGMP snooping
configuration guidelines 27-5
default configuration 28-5, 28-6

enabling
globally 27-6
on a VLAN 27-6
enabling and disabling 28-6
IP multicast and 37-4
monitoring 27-14, 28-10
overview 27-2
IGMP Snooping, displaying
group 27-16
hot membership 27-15
how to 27-15
MAC address entries 27-18
multicast router interfaces 27-17
on a VLAN interface 27-18
Querier information 27-19
IGMPSnooping Querier, configuring 27-10
Immediate Leave, IGMP
enabling 28-8
immediate-leave processing
enabling 27-8
IGMP
See fast-leave processing
ingress packets, SPAN enhancement 57-12
inline power
configuring on Cisco IP phones 43-5
insufficient inline power handling for Supervisor Engine II-TS 14-22
Intelligent Power Management 15-4
interacting with Baby Giants 8-29
interface
displaying operational status 15-6
interface command 3-9, 8-2
interface configuration
REP 24-10
interface link and trunk status events
configuring 8-37
interface port-channel command 5-45, 26-7
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 19-3
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 1-39
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 1-43
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) 1-41
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 31-3, 31-9
IOS shell
  See Auto SmartPorts macros
IP
  configuring default gateway 3-11
  configuring static routes 3-11
  displaying statistics 35-8
IP addresses
  128-bit 54-2
  cluster candidate or member 16-12
  cluster command switch 16-11
  discovering 4-44
  IPv6 54-2
ip cef command 35-6, 70-2
IP Enhanced IGRP
  interfaces, displaying 34-19
ip icmp rate-limit unreachable command 9-12
ip igmp profile command 27-31
ip igmp snooping tcn flood command 27-13
ip igmp snooping tcn flood query count command 27-14

ip igmp snooping tcn query solicit command 27-14
IP information
assigned
through DHCP-based autoconfiguration 3-2
ip load-sharing per-destination command 35-7
ip local policy route-map command 40-8
ip mask-reply command 9-13
IP MTU sizes,configuring 34-9
IP multicast
clearing table entries 37-28
configuring 37-13
default configuration 37-13
displaying PIM information 37-23
displaying the routing table information 37-24
enabling dense-mode PIM 37-15
enabling sparse-mode 37-15
features not supported 37-13
hardware forwarding 37-9
IGMP snooping and 27-5, 37-4
overview 37-1
routing protocols 37-2
software forwarding 37-9
See also Auto-RP; IGMP; PIM; RP; RPF
IP multicast routing
enabling 37-14
monitoring and maintaining 37-23
ip multicast-routing command 37-14
IP multicast traffic, load splitting 37-22
IP phones
configuring voice ports 43-3
See Cisco IP Phones 43-1
ip pim command 37-15
ip pim dense-mode command 37-15
ip pim sparse-dense-mode command 37-16
ip policy route-map command 40-7
IP Port Security for Static Hosts
on a Layer 2 access port 52-25
on a PVLAN host port 52-28
overview 52-24
ip redirects command 9-13
IP routing tables
deleting entries 37-28
IPsec VPN, introduction 1-38
IP Service Level Agreements
See IP SLAs
IP service levels, analyzing 68-1
IP SLAs
benefits 68-2
CFM endpoint discovery 65-21
configuration guidelines 68-7
Control Protocol 68-4
default configuration 68-6
definition 68-1
ICMP echo operation 68-11
manually configuring CFM ping or jitter 65-19
measuring network performance 68-3
multioperations scheduling 68-5
operation 68-3
reachability tracking 59-9
responder
described 68-4
enabling 68-7
response time 68-4
scheduling 68-5
SNMP support 68-2
supported metrics 68-2
threshold monitoring 68-6
track state 59-9
UDP jitter operation 68-8
IP Source Guard
configuring 52-20
configuring on private VLANs 52-22
displaying 52-22, 52-23
overview 52-23
IP statistics
displaying 35-8
IP traceroute
executing 9-9

overview 9-8

IP unicast

displaying statistics 35-8

IP Unnumbered support

configuring on a range of Ethernet VLANs 18-5

configuring on LAN and VLAN interfaces 18-4

configuring with connected host polling 18-6

DHCP Option 82 18-2

displaying settings 18-7

format of agent remote ID suboptions 18-2

troubleshooting 18-8

with conected host polling 18-3

with DHCP server and Relay agent 18-2

ip unreachables command 9-12

IPv4, IPv6, and MAC ACLs, configuring on a Layer 2 interface 53-29

IPv6

addresses 54-2

default configuration 54-7

defined 1-19, 54-1

Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 54-6

Router ID 54-6

OSPF 54-6

IPv6 control traffic, policing 50-16

IPv6 First Hop Security, introduction 1-39

IPX

redistribution of route information with EIGRP 1-17

is 29-19

IS-IS, introduction 1-18

ISL

trunking with 802.1Q tunneling 29-4

isolated port 44-4

isolated VLANs 44-2, 44-3, 44-4

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, 7-19

verify the software installation 5-61, 6-18, 7-18

vload the new software on standby 5-65, 6-21, 7-21

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 22-22

description 22-22

master 22-27

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 29-17
labels, definition 42-3
LACP
  system ID 26-4
Layer 2 access ports 19-7
Layer 2 Control Packet QoS
  and CoPP configuration example 50-14
  default configuation 50-11
  disabling 50-13
  enabvling 50-12
  guideline and restrictions 50-16
  understanding 50-11
Layer 2 frames
  classification with CoS 42-2
Layer 2 interface
  applying ACLs 53-31
  configuring access-mode mode on 53-31
  configuring IPv4, IPv6, and MAC ACLs 53-29
  displaying an ACL configuration 53-32
Layer 2 interfaces
  assigning VLANs 17-7
  configuring 19-5
  configuring as PVLAN host ports 44-18
  configuring as PVLAN promiscuous ports 44-17
  configuring as PVLAN trunk ports 44-19
  defaults 19-4
  disabling configuration 19-8
  modes 19-3
  show interfaces command 19-6
Layer 2 interface type
  resetting 44-24
  setting 44-24
Layer 2 protocol tunneling
  default configuration 29-16
  guidelines 29-16
Layer 2 switching
  overview 19-1
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 1-43, 9-9
  usage guidelines 9-10
Layer 2 trunks
  configuring 19-5
  overview 19-3
Layer 3 interface, applying IPv6 ACLs 53-17
Layer 3 interface counters,configuring 34-10
Layer 3 interface counters,understanding 34-3
Layer 3 interfaces
  changing from Layer 2 mode 41-16
  configuration guidelines 34-5
  configuring VLANs as interfaces 34-7
  overview 34-1
    counters 34-3
    logical 34-2
    physical 34-2
    SVI autostate exclude 34-3
Layer 3 packets
  classification methods 42-2
Layer 4 port operations
  configuration guidelines 53-11
  restrictions 53-10
Leave timer, enabling 27-9
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 24-4
Link Layer Discovery Protocol
  See CDP

link monitoring, Ethernet OAM 65-34, 65-38
link-state tracking
configuration guidelines 26-21
default configuration 26-21
described 26-18
displaying status 26-22
generic configuration procedure 26-21
link status, displaying UDLD 32-9
listening state (STP)
RSTP comparisons (table) 22-24
LLDP
configuring 31-4
characteristics 31-5
default configuration 31-5
disabling and enabling
globally 31-6
on an interface 31-7
monitoring and maintaining 31-14
overview 31-1
transmission timer and holdtime, setting 31-5
LLDP-MED
configuring
procedures 31-4
TLVs 31-9, 31-11
monitoring and maintaining 31-14
overview 31-1
supported TLVs 31-2
LLDP Media Endpoint Discovery
See LLDP-MED
load balancing
configuring for CEF 35-7
configuring for EtherChannel 26-14
overview 26-5, 35-6
per-destination 35-7
load splitting IP multicast traffic 37-22
Location Service
overview 31-1
location service
configuring 31-12
understanding 31-3
location TLV 31-3, 31-9
logging, EPM 46-129
Logical Layer 3 interfaces
configuring 34-6
logical layer 3 VLAN interfaces 34-2
login authentication
with RADIUS 46-106
with TACACS+ 3-19
login banners 4-24
login timer
changing 9-6
logoutwarning command 9-6
loop guard
and MST 22-23
configuring 25-4
overview 25-3

M

MAC/PHY configuration status TLV 31-2
MAC addresses
aging time 4-30
allocating 22-6
and VLAN association 4-29
building tables 4-28, 19-2
convert dynamic to sticky secure 49-5
default configuration 4-30
disabling learning on a VLAN 4-39
discovering 4-44
displaying 9-3
displaying in DHCP snooping binding table 52-19
dynamic
learning 4-29
removing 4-31
in ACLs 53-14
static
adding 4-37
allowing 4-38

characteristics of 4-36
dropping 4-38
removing 4-37
sticky 49-4
sticky secure, adding 49-5
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 23-10
configuring 23-10
monitoring 23-12
MAC Authentication Bypass
configure with 802.1X 46-60
MAC details, displaying 46-128
MAC extended access lists 53-14
macl 53-14
macros
See Auto SmartPorts macros
See Auto Smartports macros
See Smartports macros
MACSec
802.1AE Tagging 45-9
MACsec 45-2
configuring on an interface 45-7
defined 45-1, 45-2
switch-to-switch security 45-1
MACsec Key Agreement Protocol
See MKA
main-cpu command 11-8, 12-7
management address TLV 31-2
management options
SNMP 62-1
Management Port, Ethernet 8-6
managing software licenses, using PRTU 4-14
manual preemption, REP, configuring 24-13
marking
hardware capabilities 42-23, 42-57
marking action drivers 42-21, 42-55
marking network traffic 42-18, 42-52
marking support, multi-attribute 42-22, 42-56
match ip address command 40-6
maximum aging time (STP)
configuring 22-18
MDA
configuration guidelines 46-23 to ??
described 46-23
MEC
configuration 5-45
described 5-14
failure 5-15
Media Access Control Security
See MACsec
members
automatic discovery 16-7
member switch
managing 16-13
member switch, cluster
defined 16-2
meminfo command 73-5
messages, Ethernet OAM 65-34
messages, to users through banners 4-24
Metro features
Y.1731 (AIS and RDI), introduction 1-12
metro tags 29-2
MFIB
CEF 37-6
overview 37-12
MFIB, IP
displaying 37-26
MIBs
compiling 72-4

downloading 72-3, 72-4
overview 62-1
related information 72-3
SNMP interaction with 62-4
MKA
configuring policies 45-6
defined 45-2
policies 45-2
replay protection 45-3
statistics 45-4
virtual ports 45-3
MLD Done messages and Immediate-leave 28-4
MLD messages 28-2
MLD queries 28-3
MLD reports 28-4
MLD Snooping
MLD Done messages and Immediate-leave 28-4
MLD messages 28-2
MLD queries 28-3
MLD reports 28-4
Multicast client aging robustness 28-3
Multicast router discovery 28-3
overview 28-1
Mode of capturing control packets, selecting 53-7
modules
checking status 9-1
powering down 14-22
monitoring
802.1Q tunneling 29-18
ACL information 53-35
Ethernet CFM 65-32, 65-33
Ethernet OAM 65-49
Ethernet OAM protocol 65-49
Flex Links 23-12
IGMP
snooping 28-10
IGMP filters 27-34
IGMP snooping 27-14
Layer 2 protocol tunneling 29-18
MAC address-table move update 23-12
multicast router interfaces 28-11
multi-VRF CE 41-14, 41-21, 41-22
MVR 27-29
object tracking 59-12
REP 24-14
traffic flowing among switches 69-1
tunneling 29-18
VLAN filters 53-24
VLAN maps 53-24
monitoring and troubleshooting
BFD 39-17
M-record 22-23
MST
and multiple spanning trees 1-8, 22-22
boundary ports 22-27
BPDUs 22-23
configuration parameters 22-26
configuring 22-29
displaying configurations 22-33
edge ports 22-27
enabling 22-29
hop count 22-28
instances
configuring parameters 22-32
description 22-23
number supported 22-26
interoperability with PVST+ 22-23
link type 22-28
master 22-27
message age 22-28
regions 22-26
restrictions 22-29
to-SST interoperability 22-24
MSTP
EtherChannel guard
enabling 25-6
M-record 22-23
M-tree 22-23

M-tree 22-23
MTUS
understanding 8-26
MTU size
configuring 8-28, 8-29, 8-38
default 17-5
Multi-authentication
described 46-23
multiauthentication mode 46-8
multicast
See IP multicast
Multicast client aging robustness 28-3
multicast Ethernet loopback, using 65-31
multicast Ethernet loopback (ETH-LB) 65-29
Multicast Forwarding Information Base (MFIB) 37-12
multicast groups
static joins 28-7
Multicast HA 37-13
Multicast implementation
HA 37-13
MFIB 37-12
S/M, 224/4 37-13
multicast packets
blocking 55-2
Multicast router discovery 28-3
multicast router interfaces, displaying 27-17
multicast router interfaces, monitoring 28-11
multicast router ports, adding 28-7
multicast routers
flood suppression 27-12
multicast router table
displaying 37-24
Multicast Storm Control
enabling 56-4
disabling 56-5
multicast television application, using MVR 27-21
Multicast VLAN Registration
See MVR
multichassis EtherChannel
see MEC 5-14
multidomain authentication
See MDA
multidomain authentication mode 46-7
multioperations scheduling, IP SLAs 68-5
Multiple AuthorizationAuthentication
configuring 46-34
Multiple Domain Authentication 46-34
multiple forwarding paths 1-8, 22-22
multiple-hosts mode 46-7
Multiple Spanning Tree
See MST
multiple VPN routing/forwarding
See multi-VRF CE
multi-VRF CE
components 41-3
configuration example 41-17
defined 41-1
displaying 41-14, 41-21, 41-22
monitoring 41-14, 41-21, 41-22
network components 41-3
packet-forwarding process 41-3
MVR
configuration guidelines and limitations 27-23
configuring global parameters 27-24
configuring on access ports 27-26
configuring on a trunk port 27-27
default configuration 27-23
displaying information 27-29
in a multicast television application 27-21
monitoring 27-29
setting global parameters 27-24

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 53-16
named MAC extended ACLs
ACLs
configuring named MAC extended 53-14, 53-15
native VLAN
and 802.1Q tunneling 29-4
specifying 19-5
NDAC 45-9
defined 45-9
MACsec 45-1
NEAT
configuring 46-88
overview 46-24
neighbor offset numbers, REP 24-5
NetFlow-lite
clear commands 63-9
display commands 63-8
NetFlow packet sampling
about 63-2
Network Assistant
and VTY 16-12
configure
enable communication with switch 16-13, 16-17
default configuration 16-3
overview of CLI commands 16-3
Network Device Admission Control (NDAC) 45-9
Network Edge Access Topology
See NEAT
network fault tolerance 1-8, 22-22
network management
configuring 30-1
RMON 69-1
SNMP 62-1
network performance, measuring with IP SLAs 68-3
network policy TLV 31-2, 31-9
Network Time Protocol
See NTP
network traffic, marking 42-18, 42-52
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 32-7
non-IP traffic filtering 53-14, 53-15
non-RPF traffic
description 37-10
in redundant configurations (figure) 37-11
Nonstop Forwarding
See NSF
nonvolatile random-access memory
See NVRAM
normal-range VLANs
See VLANs
NSF
defined 13-1
guidelines and restrictions 13-9
operation 13-4
NSF-aware
supervisor engines 13-3
support 13-2
NSF-capable
supervisor engines 13-3
support 13-2
NSF with SSO supervisor engine redundancy
and CEF 13-5
overview 13-3
SSO operation 13-4
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 65-34
features 65-34
sublayer 65-34
OAM manager
configuring 65-52
with CFM and Ethernet OAM 65-51
OAM PDUs 65-35
OAM protocol data units 65-33
OBFL, displaying for the 9000W AC 14-4
object tracking
monitoring 59-12
OIR
overview 8-33
on-demaind online diagnostics 70-2
online diagnostic
troubleshooting 70-8
Online Diagnostics 70-1
online diagnostics
configuring on-demaind 70-2
data path, displaying test results 70-7
displaying tests and test results 70-4
linecard 70-8
scheduling 70-2
starting and stopping tests 70-3
online insertion and removal
See OIR
Open Shortest Path First
See OSPF
operating system images
See system images
Option 82
enabling DHCP Snooping 52-10
OSPF
area concept 1-18
description 1-18
for IPv6 54-6
OSPF, introduction 1-18
OSPF for Routed Access, introduction 1-21

P

packets
modifying 42-9
packet type filtering
overview 57-14
SPAN enhancement 57-14
PACL
using with access-group mode 53-30
PACL configuration guidelines 53-28
PACL with VLAN maps and router ACLs 53-32
PAgP
understanding 26-4
PAgP, dual-active detection 5-23
passwords
configuring enable password 3-14
configuring enable secret password 3-14

encrypting 3-22
in clusters 16-8
recovering lost enable password 3-25
setting line password 3-14
PBR (policy-based routing)
configuration (example) 40-8
enabling 40-6
features 40-2
overview 40-1
route-map processing logic 40-3
route-map processing logic example 40-4
route maps 40-2
when to use 40-5
percentage thresholds in tracked lists 59-6
Permanent Right-To_Use 4-14
per-port and VLAN Access Control List 52-19
per-port per-VLAN QoS
enabling 42-36, 42-70
overview 42-10
Per-User ACL and Filter-ID ACL, configure 46-45
Per-VLAN Rapid Spanning Tree 22-6
enabling 22-20
overview 22-6
PE to CE routing, configuring 41-9
physical layer 3 interfaces 34-2
Physical Layer 3 interfaces, configuring 34-12
PIM
configuring dense mode 37-15
configuring sparse mode 37-15
displaying information 37-23
displaying statistics 37-27
enabling sparse-dense mode 37-15, 37-16
overview 37-3
PIM-DM 37-3
PIM on an interface, enabling 37-14
PIM-SM 37-3
PIM-SSM mapping, enabling 37-17
ping
executing 9-8
overview 9-7
ping command 9-8, 37-23
PoE 15-7, 15-8
configuring power consumption, powered devices 15-5
configuring power consumption for single device 15-5, 15-16
displaying operational status for an interface 15-6
Enhanced PoE support on E-series 15-15
policing and monitoring 15-12
power consumption for powered devices
Intelligent Power Management 15-4
powering down a module 14-22
power management modes 15-2
PoE policing
configuring errdisable recovery 15-14
configuring on an interface 15-13
displaying on an interface 15-14
power modes 15-12
point-to-point
in 802.1X authentication (figure) 46-3
policing
how to implement 42-18, 42-52
See QoS policing
policing, PoE 15-12
policing IPv6 control traffic 50-16
policy associations, QoS on Sup 6-E 42-39, 42-73
policy-map command 42-16, 42-51
policy map marking action, configuring 42-23, 42-57
port ACLs
and voice VLAN 53-4
defined 53-3
Port Aggregation Protocol
see PAgP
port-based authentication
802.1X with voice VLAN 46-22
Authentication Failed VLAN assignment 46-17
authentication server
defined 48-2

changing the quiet period 46-84
client, defined 46-3, 48-2
configuration guidelines 46-29, 48-6
configure ACL assignments and redirect URLs 46-38
configure switch-to-RADIUS server communication 46-32
configure with Authentication Failed 46-70
configure with Critical Authentication 46-62
configure with Guest-VLANs 46-57
configure with MAC Authentication Bypass 46-60
configure with VLAN User Distribution 46-68
configure with Voice VLAN 46-72
configuring
  Multiple Domain Authentication and Multiple Authorization 46-34
  RADIUS server 48-10
  RADIUS server parameters on the switch 48-9
configuring Fallback Authentication 46-77
configuring Guest-VLAN 46-32
configuring manual re-authentication of a client 46-94
configuring with Unidirectional Controlled Port 46-66
controlling authorization state 46-5
default configuration 46-27, 48-6
described 46-1
device roles 46-2, 48-2
displaying statistics 46-125, 48-14
enabling 46-29
  802.1X authentication 48-9
enabling multiple hosts 46-83
enabling periodic re-authentication 46-81
encapsulation 46-3
host mode 46-6
how 802.1X fails on a port 46-25
initiation and message exchange 46-4
method lists 46-29
modes 46-6
multidomain authentication 46-23
multiple-hosts mode, described 46-7
port security
  multiple-hosts mode 46-7
ports not supported 46-5
pre-authentication open access 46-8
resetting to default values 46-95
setting retransmission number 46-86
setting retransmission time 46-85
switch
  as proxy 48-2
switch supplicant
  configuring 46-88
  overview 46-24
topologies, supported 46-26
using with ACL assignments and redirect URLs 46-20
using with port security 46-19
voice aware 802.1x security
  configuring 46-74
  described 46-22, 46-73
with Critical Authentication 46-14
with Guest VLANs 46-11
with MAC Authentication Bypass 46-12
with Unidirectional Controlled Port 46-15
with VLAN assignment 46-10
with VLAN User Distribution 46-16
port-channel
  see EtherChannel
port-channel interfaces
  See also EtherChannel
  creating 5-45, 26-7
  overview 26-2
port-channel load-balance
  command 26-13
  command example 26-13
port-channel load-balance command 26-14
port cost (STP)
  configuring 22-15
port description TLV 31-2
PortFast

and MST 22-23
BPDU filter, configuring 25-9
configuring or enabling 25-15
overview 25-6
PortFast BPDU filtering
and MST 22-23
enabling 25-9
overview 25-9
port numbering with TwinGig Convertors 8-13
port priority
configuring MST instances 22-32
configuring STP 22-13
ports
blocking 55-1
checking status 9-2
dynamic VLAN membership
example 17-29
reconfirming 17-26
forwarding, resuming 55-3
REP 24-6
See also interfaces
port security
aging 49-5
configuring 49-7
displaying 49-28
guidelines and restrictions 49-33
on access ports 49-7, 49-22
on private VLAN 49-14
host 49-14
promiscuous 49-16
topology 49-15, 49-18, 49-32
on trunk port 49-17
guidelines and restrictions 49-15, 49-18, 49-32
port mode changes 49-22
on voice ports 49-22
sticky learning 49-5
using with 802.1X 46-19
violations 49-6
with 802.1X Authentication 49-32
with DHCP and IP Source Guard 49-31
with other features 49-33
port states
description 22-5
port VLAN ID TLV 31-2
power
inline 43-5
power dc input command 14-21
powered devices, configuring power consumption 15-5
power handling for Supervisor Engine II-TS 15-12
power inline command 15-3
power inline consumption command 15-5
power management
Catalyst 4500 series 14-7
Catalyst 4500 Switch power supplies 14-14
Catalyst 4948 series 14-23
configuring combined mode 14-13
configuring redundant mode 14-12
overview 14-1
redundancy 14-7
power management for Catalyst 4500 Switch
combined mode 14-9
redundant mode 14-9
power management limitations in Catalyst 4500 Switch 14-10
power management mode
selecting 14-10
power management TLV 31-2, 31-3, 31-9
power negotiation
through LLDP 31-11
Power-On-Self-Test diagnostics 70-10, 70-20
Power-On-Self-Test for Supervisor Engine V-10GE 70-13
power policing, displaying on an interface 15-14
power redundancy-mode command 14-13
power supplies
available power for Catalyst 4500 Switch 14-14
fixed 14-8
variable 14-8, 14-23

pre-authentication open access 46-8
pre-authentication open access. See port-based authentication.
preempt delay time, REP 24-5
primary edge port, REP 24-4
primary VLANs 44-2, 44-4
  associating with secondary VLANs 44-16
  configuring as a PVLAN 44-15
priority
  overriding CoS of incoming frames 43-5
priority queuing, QoS on Sup 6-E 42-30, 42-64
private VLAN
  configure port security 49-14, 49-15
  enabling DHCP Snooping 52-12
private VLANs
  across multiple switches 44-5
  and SVIs 44-10
  benefits of 44-2
  community ports 44-3
  community VLANs 44-2, 44-3
  default configuration 44-12
  end station access to 44-3
  isolated port 44-4
  isolated VLANs 44-2, 44-3, 44-4
  ports
    community 44-3
    isolated 44-4
    promiscuous 44-4
  primary VLANs 44-2, 44-4
  promiscuous ports 44-4
  secondary VLANs 44-2
  subdomains 44-2
  traffic in 44-9
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 44-17
  defined 44-4
  setting mode 44-24
protocol timers 22-4
provider edge devices 41-2
PRTU, managing software licenses 4-14
pruning, VTP
  See VTP pruning
pseudobridges
  description 22-25
PVACL 52-19
PVID (port VLAN ID)
  and 802.1X with voice VLAN ports 46-22
PVLAN promiscuous trunk port
  configuring 44-11, 44-17, 44-21
PVLANs
  802.1q support 44-14
  across multiple switches 44-5
  configuration guidelines 44-12
  configure port security 49-14, 49-16, 49-18
  configure port security in a wireless setting 49-32
  configuring 44-11
  configuring a VLAN 44-15
  configuring promiscuous ports 44-17
  host ports
    configuring a Layer 2 interface 44-18
    setting 44-24
  overview 44-1
  permitting routing, example 44-23
  promiscuous mode
    setting 44-24
  setting
    interface mode 44-24

Q

QoS
  classification 42-6 to ??

definitions 42-3
enabling per-port per-VLAN 42-36, 42-70
overview 42-1
overview of per-port per-VLAN 42-10
packet modification 42-9
traffic shaping 42-9
See also COS; DSCP values; transmit queues
QoS active queue management
tracking queue length 42-9
QoS labels
definition 42-3
QoS marking
description 42-5
QoS on Sup 6-E
Active Queue management via DBL 42-34, 42-68
active queue management via DBL 42-27, 42-34, 42-61, 42-68
classification 42-16, 42-50
configuring 42-13, 42-47
configuring CoS mutation 42-45, 42-79
configuring the policy map marking action 42-23, 42-57
hardware capabilities for marking 42-23, 42-57
how to implement policing 42-18, 42-52
marking action drivers 42-21, 42-55
marking network traffic 42-18, 42-52
MQC-based QoS configuration 42-13, 42-48
multi-attribute marking support 42-22, 42-56
platform hardware capabilities 42-15, 42-49
platform restrictions 42-18, 42-52
platform-supported classification criteria and QoS features 42-13, 42-14, 42-48
policing 42-17, 42-51
policy associations 42-39, 42-73
prerequisites for applying a service policy 42-15, 42-49
priority queuing 42-30, 42-64
queue-limiting 42-31, 42-65
restrictions for applying a service policy 42-15, 42-50
shaping 42-25, 42-59
sharing(bandwidth) 42-27, 42-61
sharing(blandwidth), shapring, and priority queuing 42-25, 42-59
software QoS 42-40, 42-74
traffic marking procedure flowchart 42-21, 42-55
QoS policing
definition 42-5
described 42-8
QoS policy
attaching to interfaces 42-8
QoS service policy
prerequisites 42-15, 42-49
restrictions for applying 42-15, 42-50
QoS transmit queues
burst 42-9
maximum rate 42-9
sharing link bandwidth 42-9
quad-supervisor
uplink forwarding 5-6
Quality of service
See QoS
queueing 42-8
queue-limiting, QoS on Sup 6-E 42-31, 42-65

R

RADIUS
attributes
vendor-proprietary 46-114
vendor-specific 46-112
change of authorization 46-97
configuring
accounting 46-111
authentication 46-106
authorization 46-110
communication, global 46-104, 46-112
communication, per-server 46-103, 46-104
multiple UDP ports 46-104
default configuration 46-103
defining AAA server groups 46-108

displaying the configuration 46-116
identifying the server 46-103
limiting the services to the user 46-110
method list, defined 46-103
operation of 46-97
server load balancing 46-116
suggested network environments 46-96
tracking services accessed by user 46-111
understanding 46-96
RADIUS, controlling switch access with 46-95
RADIUS Change of Authorization 46-97
RADIUS server
configure to-Switch communication 46-32
configuring settings 46-34
parameters on the switch 46-32
RA Guard
configuring 53-36
deployment 53-36
examples 53-37
introduction 53-35
usage guidelines 53-38
range command 8-4
range macros
defining 8-11
ranges of interfaces
configuring 8-4
Rapid Spanning Tree
See RSTP
rcommand command 16-13
reachability, tracking IP SLAs IP host 59-9
re-authentication of a client
configuring manual 46-94
enabling periodic 46-81
redirect URLs, port-based authentication 46-20
reduced MAC address 22-2
redundancy
configuring 11-7, 12-7
guidelines and restrictions 11-5, 12-5
changes made through SNMP 11-11, 12-11
NSF-aware support 13-2
NSF-capable support 13-2
overview 11-2, 12-2
redundancy command 11-8, 12-7
understanding synchronization 11-4, 12-5
redundancy (NSF) 13-1
configuring
BGP 13-11
CEF 13-10
EIGRP 13-16
IS-IS 13-13
OSPF 13-12
routing protocols 13-5
redundancy (RPR)
route processor redundancy 11-2, 12-3
synchronization 11-5, 12-5
redundancy (SSO)
redundancy command 13-10
route processor redundancy 11-3, 12-3
synchronization 11-5, 12-5
reload command 3-28, 3-29
Remote Authentication Dial-In User Service
See RADIUS
remote failure indications 65-34
remote loopback, Ethernet OAM 65-34, 65-37
Remote Network Monitoring
See RMON
rendezvous point, configuring 37-17
rendezvous point, configuring single static 37-20
REP
administrative VLAN 24-8
administrative VLAN, configuring 24-9
and STP 24-6
configuration guidelines 24-7
configuring interfaces 24-10
convergence 24-4
default configuration 24-7
manual preemption, configuring 24-13
monitoring 24-14

neighbor offset numbers 24-5
open segment 24-2
ports 24-6
preempt delay time 24-5
primary edge port 24-4
ring segment 24-2
secondary edge port 24-4
segments 24-1
characteristics 24-2
SNMP traps, configuring 24-14
supported interfaces 24-1
triggering VLAN load balancing 24-6
verifying link integrity 24-4
VLAN blocking 24-13
VLAN load balancing 24-4
replication
description 37-9
report suppression, IGMP
disabling 28-10
reserved-range VLANs
See VLANs
reset command 73-3
resetting an interface to default configuration 8-40
resetting a switch to defaults 3-32
Resilient Ethernet ProtocolLSee REP
responder, IP SLAs
described 68-4
enabling 68-7
response time, measuring with IP SLAs 68-4
restricting access
NTP services 4-8
RADIUS 46-95
TACACS+ 3-15
retransmission number
setting in 802.1X authentication 46-86
retransmission time
changing in 802.1X authentication 46-85
RFC
1157, SNMPv1 62-2
1305, NTP 4-2
1757, RMON 69-2
1901, SNMPv2C 62-2
1902 to 1907, SNMPv2 62-2
2273-2275, SNMPv3 62-2
RFC 5176 Compliance 46-98
RIP
description 1-19
for IPv6 54-5
RIP, introduction 1-19
RMON
default configuration 69-3
displaying status 69-6
enabling alarms and events 69-3
groups supported 69-2
overview 69-1
ROM monitor
boot process and 3-26
CLI 2-7
commands 73-2 to 73-3
debug commands 73-5
entering 73-1
exiting 73-6
overview 73-1
root bridge
configuring 22-9
selecting in MST 22-22
root guard
and MST 22-23
enabling 25-2
overview 25-2
routed packets
ACLs 53-26
route-map (IP) command 40-6
route maps
defining 40-6
PBR 40-2
router ACLs
description 1-41, 53-3

using with VLAN maps 53-25
router ACLs, using PACL with VLAN maps 53-32
route targets
VPN 41-3
Routing Information Protocol
See RIP
RPF
See Unicast RPF
RSPAN
configuration guidelines 57-16
destination ports 57-5
IDS 57-2
monitored ports 57-4
monitoring ports 57-5
received traffic 57-3
sessions
creating 57-17
defined 57-3
limiting source traffic to specific VLANs 57-23
monitoring VLANs 57-21
removing source (monitored) ports 57-20
specifying monitored ports 57-17
source ports 57-4
transmitted traffic 57-4
VLAN-based 57-5
RSTP
compatibility 22-23
description 22-22
port roles 22-24
port states 22-24

S

S/M, 224/4 37-13
SAID
See 802.10 SAID
SAP
defined 45-9
negotiation 45-9
support 45-1
scheduling 42-8
scheduling, IP SLAs operations 68-5
secondary edge port, REP 24-4
secondary root switch 22-12
secondary VLANs 44-2
associating with primary 44-16
permitting routing 44-23
security
configuring 50-1
Security Association Identifier
See 802.10 SAID
Security Exchange Protocol
See SXP
Security Exchange Protocol
See SAP
selecting a power management mode 14-10
selecting X2/TwinGig Convertor Mode 8-14
sequence numbers in log messages 60-7
server IDs
description 67-23
service policy, configure class-level queue-limit 42-31, 42-65
service-policy input command 33-2
service-provider networks
and customer VLANs 29-2
session keys, MKA 45-2
set default interface command 40-7
set interface command 40-7
set ip default next-hop command 40-7
set ip next-hop command 40-6
set-request operation 62-4
severity levels, defining in system messages 60-8
shaping, QoS on Sup 6-E 42-25, 42-59
sharing(bandwidth), QoS on Sup 6-E 42-27, 42-61
Shell functions
See Auto SmartPorts macros
See Auto Smartports macros
Shell triggers

See Auto SmartPorts macros
See Auto Smartports macros
show adjacency command 35-9
show boot command 3-32
show catalyst4000 chassis-mac-address command 22-3
show cdp command 30-2, 30-3
show cdp entry command 30-4
show cdp interface command 30-3
show cdp neighbors command 30-4
show cdp traffic command 30-4
show ciscoview package command 4-48
show ciscoview version command 4-48
show cluster members command 16-13
show configuration command 8-23
show debugging command 30-4
show environment command 14-2
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 35-8
show ip eigrp interfaces command 34-19
show ip eigrp neighbors command 34-19
show ip eigrp topology command 34-19
show ip eigrp traffic command 34-19
show ip interface command 37-23
show ip local policy command 40-8
show ip mroute command 37-23
show ip pim interface command 37-23
show l2protocol command 29-18
show lldp traffic command 31-15
show mac-address-table address command 9-3
show mac-address-table interface command 9-3
show mls entry command 35-8
show module command 9-1, 22-6
show PoE consumed 15-8
show power inline command 15-6
show power supplies command 14-13
show protocols command 8-36
show running-config command
adding description for an interface 8-23
checking your settings 3-9
displaying ACLs 53-19, 53-21, 53-30, 53-31
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 29-16
shutting down
interfaces 8-37
Simple Network Management Protocol
See SNMP
single-host mode 46-7
single spanning tree
See SST
single static RP, configuring 37-20
slot numbers, description 8-2
Slow timer, configuring BFD 39-16
smart call home 67-1
description 67-2
destination profile (note) 67-5
registration requirements 67-3
service contract requirements 67-3
Transport Gateway (TG) aggregation point 67-2
SMARTnet
smart call home registration 67-3
Smartports macros
applying global parameter values 20-8, 20-15
applying macros 20-8
applying parameter values 20-9
configuration guidelines 20-6, 20-14
configuring 20-2
creating 20-8
default configuration 20-4, 20-13
defined 1-10, 20-1
displaying 20-13
tracing 20-7, 20-14
SNMP
accessing MIB variables with 62-4

agent
described 62-4
disabling 62-7
and IP SLAs 68-2
authentication level 62-10
community strings
configuring 62-7
overview 62-4
configuration examples 62-15
configuration guidelines 62-6
default configuration 62-5
enabling 72-4, 72-5
engine ID 62-6
groups 62-6, 62-9
host 62-6
informs
and trap keyword 62-11
described 62-5
differences from traps 62-5
enabling 62-14
limiting access by TFTP servers 62-15
limiting system log messages to NMS 60-9
manager functions 62-3
notifications 62-5
overview 62-1, 62-4
status, displaying 62-16
system contact and location 62-14
trap manager, configuring 62-13
traps
described 62-3, 62-5
differences from informs 62-5
enabling 62-11
enabling MAC address notification 4-31
enabling MAC move notification 4-33
enabling MAC threshold notification 4-35
overview 62-1, 62-4
types of 62-11
users 62-6, 62-9
versions supported 62-2
SNMP commands 72-4
SNMP traps
REP 24-14
SNMPv1 62-2
SNMPv2C 62-2
SNMPv3 62-2
software
upgrading 11-13, 12-12
software configuration register 3-26
software QoS, on Sup 6-E 42-40, 42-74
software switching
description 35-5
interfaces 35-6
key data structures used 37-8
source IDs
call home event format 67-22
SPAN
and ACLs 57-5
configuration guidelines 57-7
configuring 57-6 to 57-10
destination ports 57-5
IDS 57-2
monitored port, defined 57-4
monitoring port, defined 57-5
received traffic 57-3
sessions
defined 57-3
source ports 57-4
transmitted traffic 57-4
VLAN-based 57-5
SPAN and RSPAN
concepts and terminology 57-3
default configuration 57-6
displaying status 57-24
overview 57-1
session limits 57-6
SPAN enhancements
access list filtering 57-13
configuration example 57-15

CPU port sniffing 57-10
encapsulation configuration 57-12
ingress packets 57-12
packet type filtering 57-14
spanning-tree backbonefast command 25-16
spanning-tree cost command 22-15
spanning-tree guard root command 25-2
spanning-tree portfast bpdu-guard command 25-8
spanning-tree portfast command 25-7
spanning-tree port-priority command 22-13
spanning-tree uplinkfast command 25-12
spanning-tree vlan
command 22-9
command example 22-9
spanning-tree vlan command 22-8
spanning-tree vlan cost command 22-16
spanning-tree vlan forward-time command 22-19
spanning-tree vlan hello-time command 22-18
spanning-tree vlan max-age command 22-18
spanning-tree vlan port-priority command 22-13
spanning-tree vlan priority command 22-17
spanning-tree vlan root primary command 22-10
spanning-tree vlan root secondary command 22-12
speed
configuring interface 8-20
speed command 8-21
SSO
configuring 13-10
SSO operation 13-4
SST
description 22-22
interoperability 22-24
static ACL, removing the requirement 53-28
static addresses
See addresses
static routes
configuring 3-11
verifying 3-12
statistics
802.1X 48-14
displaying 802.1X 46-125
displaying PIM 37-27
LLDP 31-14
LLDP-MED 31-14
MKA 45-4
SNMP input and output 62-16
sticky learning
configuration file 49-6
defined 49-5
disabling 49-6
enabling 49-5
saving addresses 49-6
sticky MAC addresses
configuring 49-7
defined 49-4
storing captured packets to a .pcap file, Wireshark 58-8
Storm Control
displaying 56-6
enabling Broadcast 56-3
enabling Multicast 56-4
hardware-based, implementing 56-2
overview 56-1
software-based, implementing 56-2
STP
and REP 24-6
bridge ID 22-2
configuring 22-7 to 22-20
creating topology 22-5
defaults 22-7
disabling 22-20
enabling 22-8
enabling extended system ID 22-9
enabling Per-VLAN Rapid Spanning Tree 22-20
EtherChannel guard
disabling 25-6
forward-delay time 22-19
hello time 22-17
Layer 2 protocol tunneling 29-13

maximum aging time 22-18
overview 22-1, 22-3
per-VLAN rapid spanning tree 22-6
port cost 22-15
port priority 22-13
root bridge 22-9
stratum, NTP 4-2
stub routing (EIGRP)
benefits 34-17
configuration tasks 34-18
configuring 34-14
overview 34-13, 34-14
restrictions 34-17
verifying 34-18
subdomains, private VLAN 44-2
summer time 4-13
supervisor engine
accessing the redundant 11-14, 12-14
configuring 3-8 to 3-13
copying files to standby 11-14, 12-14
default configuration 3-1
default gateways 3-11
environmental monitoring 14-1
redundancy 13-1
ROM monitor 3-26
startup configuration 3-25
static routes 3-11
synchronizing configurations 11-11, 12-10
Supervisor Engine 7L-E, selecting the uplink port 8-18
Supervisor Engine II-TS
insufficient inline power handling 14-22, 15-12
Smartports macros
See also Auto Smartports macros
SVI Autostate Exclude
understanding 34-3
SVI Autostate exclude
configuring 34-7
S-VLAN 1-2, 29-7
switch 54-2
switch access with RADIUS, controlling 46-95
switched packets
and ACLs 53-25
Switched Port Analyzer
See SPAN
switchport
show interfaces 8-28, 8-29, 8-38
switchport access vlan command 19-5, 19-7
switchport block multicast command 55-2
switchport block unicast command 55-2
switchport mode access command 19-7
switchport mode dot1q-tunnel command 29-6
switchport mode dynamic command 19-5
switchport mode trunk command 19-5
switch ports
See access ports
switchport trunk allowed vlan command 19-5
switchport trunk encapsulation command 19-5
switchport trunk native vlan command 19-5
switchport trunk pruning vlan command 19-6
switch-to-RADIUS server communication
configuring 46-32
sysret command 73-5
system
reviewing configuration 3-10
settings at startup 3-27
system alarms
overview 14-6
system and network statistics, displaying 37-23
system capabilities TLV 31-2
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 31-2
system images
loading from Flash memory 3-30
modifying boot field 3-27
specifying 3-30
system message logging
default configuration 60-3
defining error message severity levels 60-8
disabling 60-4
displaying the configuration 60-12
enabling 60-4
facility keywords, described 60-12
level keywords, described 60-9
limiting messages 60-9
message format 60-2
overview 60-1
sequence numbers, enabling and disabling 60-7
setting the display destination device 60-5
synchronizing log messages 60-6
timestamps, enabling and disabling 60-7
UNIX syslog servers
configuring the daemon 60-10
configuring the logging facility 60-11
facilities supported 60-12
system MTU
802.1Q tunneling 29-5
maximums 29-5
system name
manual configuration 4-22
See also DNS
system name TLV 31-2
system prompt, default setting 4-21

T

TACACS+ 50-1
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 29-3
Layer 2 protocol 29-13
TCAM programming and ACLs 53-7
for Sup II-Plust thru V-10GE 53-6
TCAM programming and ACLs for Sup 6-E 53-10
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 65-45
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 62-15
TFTP download
See also console download
threshold monitoring, IP SLAs 68-6
time

See NTP and system clock
Time Domain Reflectometer
See TDR
time exceeded messages 9-9
timer
See login timer
timestamps in log messages 60-7
time zones 4-12
TLV
host presence detection 46-8
TLVs
defined 1-7, 31-2
LLDP-MED 31-2
Token Ring
media not supported (note) 17-5, 17-10
Topology change notification processing
MLD Snooping
Topology change notification processing 28-4
TOS
description 42-4
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 59-3
types 59-3
tracked objects
by Boolean expression 59-4
by threshold percentage 59-6
by threshold weight 59-5
tracking interface line-protocol state 59-2
tracking IP routing state 59-2
tracking objects 59-1
tracking process 59-1
track state, tracking IP SLAs 59-9
traffic
blocking flooded 55-2
traffic control
using ACLs (figure) 53-4
using VLAN maps (figure) 53-5
traffic marking procedure flowchart 42-21, 42-55
traffic shaping 42-9
translational bridge numbers (defaults) 17-5
traps
configuring MAC address notification 4-31
configuring MAC move notification 4-33
configuring MAC threshold notification 4-35
configuring managers 62-11
defined 62-3
enabling 4-31, 4-33, 4-35, 62-11
notification types 62-11
overview 62-1, 62-4
troubleshooting
with CiscoWorks 62-4
with system message logging 60-1
with traceroute 9-8
troubleshooting high CPU due to ACLs 53-6
trunk failover
See link-state tracking
trunk ports
configure port security 49-17
configuring PVLAN 44-19 to 44-21
trunks
802.1Q restrictions 19-4
configuring 19-5
configuring access VLANs 19-5
configuring allowed VLANs 19-5
default interface configuration 19-5
enabling to non-DTP device 19-3
specifying native VLAN 19-5
understanding 19-3
trustpoint 67-3
tunneling
defined 29-1
tunnel ports

802.1Q, configuring 29-6
described 29-2
incompatibilities with other features 29-5
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 32-8
default configuration 32-4
disabling on fiber-optic interfaces 32-7
disabling on non-fiber-optic interfaces 32-7
displaying link status 32-9
enabling globally 32-5
enabling per-interface 32-6
modes of operation 32-3
resetting disabled LAN interfaces 32-8
use case 32-2
UDLD, overview 32-1
UDP jitter, configuring 68-9
UDP jitter operation, IP SLAs 68-8
unauthorized ports with 802.1X 46-5
unicast
See IP unicast
unicast flood blocking
configuring 55-1
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 53-13
Unicast RPF (Unicast Reverse Path Forwarding)
applying 36-5
BGP attributes
caution 36-4
CEF
requirement 36-2
tables 36-7
configuring 36-9
(examples) ?? to 36-12
BOOTP 36-8
DHCP 36-8
enterprise network (figure) 36-6
prerequisites 36-9
routing table requirements 36-7
tasks 36-9
verifying 36-10
deploying 36-5
description 1-22, 36-1
disabling 36-11
enterprise network (figure) 36-6
FIB 36-2
implementing 36-4
packets, dropping (figure) 36-4
prerequisites 36-9
restrictions
basic 36-8
routing asymmetry 36-7
routing asymmetry (figure) 36-8
routing table requirements 36-7
security policy
applying 36-5
attacks, mitigating 36-5
deploying 36-5

tunneling 36-5
source addresses, validating 36-3
(figure) 36-3, 36-4
failure 36-3
traffic filtering 36-5
tunneling 36-5
validation
failure 36-3, 36-4
packets, dropping 36-3
source addresses 36-3
verifying 36-10
unicast traffic
blocking 55-2
Unidirectional Controlled Port, configuring 802.1X 46-66
unidirectional ethernet
enabling 33-2
example of setting 33-2
overview 33-1
UniDirectional Link Detection Protocol
See UDLD
Universal PoE, configuring 15-16
UNIX syslog servers
daemon configuration 60-10
facilities supported 60-12
message logging configuration 60-11
UplinkFast
and MST 22-23
enabling 25-15
MST and 22-23
overview 25-11
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 58-18
user-defined event triggers
configuring, 802.1X-based 21-8
configuring, MAC address-based 21-9
User-defined triggers and built-in macros, configuring mapping 21-9
user EXEC mode 2-5
user sessions
disconnecting 9-7
monitoring 9-6

V

VACLs
Layer 4 port operations 53-10
virtual configuration register 73-3
virtual LANs
See VLANs
virtual ports, MKA 45-3
Virtual Router Redundancy Protocol, introduction 1-22
Virtual Switch System(VSS), displaying EtherChannel to 26-16
VLAN ACLs
See VLAN maps
VLAN blocking, REP 24-13
vlan command 17-6
vlan dot1q tag native command 29-4
VLAN ID
service provider 29-9
VLAN ID, discovering 4-44
VLAN ID translation
See VLAN mapping
VLAN load balancing
REP 24-4
VLAN load balancing, triggering 24-6
VLAN load balancing on flex links 23-2
configuration guidelines 23-6
VLAN Management Policy Server
See VMPS
VLAN mapping
1-to-1 29-8
1-to-1, configuring 29-11
configuration guidelines 29-10

configuring 29-11
configuring on a trunk port 29-11
default 29-9
described 1-2, 29-7
selective QinQ 29-8
selective Q-in-Q, configuring 29-12
traditional QinQ 29-8
traditional Q-in-Q, configuring 29-12
types of 29-8
VLAN maps
applying to a VLAN 53-21
configuration example 53-22
configuration guidelines 53-18
configuring 53-17
creating and deleting entries 53-19
defined 1-41
denying access example 53-23
denying packets 53-19
displaying 53-24
order of entries 53-18
permitting packets 53-19
router ACLs and 53-25
using (figure) 53-5
using in your network 53-22
VLAN maps, PACL and Router ACLs 53-32
VLANs
allowed on trunk 19-5
configuration guidelines 17-3
configuring 17-5
configuring as Layer 3 interfaces 34-7
customer numbering in service-provider networks 29-3
default configuration 17-4
description 1-11
extended range 17-3
IDs (default) 17-5
interface assignment 17-7
limiting source traffic with RSPAN 57-23
monitoring with RSPAN 57-21
name (default) 17-5
normal range 17-3
overview 17-1
reserved range 17-3
See also PVLANs
VLAN Trunking Protocol
See VTP
VLAN trunks
overview 19-3
VLAN User Distribution, configuring 802.1X 46-68
VMPS
configuration file example 17-32
configuring dynamic access ports on client 17-25
configuring retry interval 17-27
database configuration file 17-32
dynamic port membership
example 17-29
reconfirming 17-26
reconfirming assignments 17-26
reconfirming membership interval 17-26
server overview 17-21
VMPS client
administering and monitoring 17-27
configure switch
configure reconfirmation interval 17-26
dynamic ports 17-25
entering IP VMPS address 17-24
reconfirmation interval 17-27
reconfirm VLAM membership 17-26
default configuration 17-24
dynamic VLAN membership overview 17-23
troubleshooting dynamic port VLAN membership 17-28
VMPS server
fall-back VLAN 17-22
illegal VMPS client requests 17-23
overview 17-21
security modes
multiple 17-22

open 17-21
secure 17-22
voice aware 802.1x security
port-based authentication
configuring 46-74
described 46-22, 46-73
voice interfaces
configuring 43-1
Voice over IP
configuring 43-1
voice ports
configuring VVID 43-3
voice traffic 15-2, 43-5
voice VLAN
IP phone data traffic, described 43-2
IP phone voice traffic, described 43-2
Voice VLAN, configure 802.1X 46-72
voice VLAN ports
using 802.1X 46-22
VPN
configuring routing in 41-8
forwarding 41-3
routes 41-2
routing and forwarding table
See VRF
VRF
defining 41-3
tables 41-1
VRF-aware services
ARP 41-6, 41-15, 41-17
configuring 41-6, 41-15
ftp 41-16
ping 41-15
tftp 41-16
traceroute 41-16
uRPF 41-16
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 17-16
configuration guidelines 17-12
default configuration 17-13
disabling 17-16
Layer 2 protocol tunneling 29-14
monitoring 17-19
overview 17-8
pruning
configuring 17-15
See also VTP version 2
server, configuring 17-16
statistics 17-19
transparent mode, configuring 17-16
version 2
enabling 17-15
VTP advertisements
description 17-9
VTP domains
description 17-8
VTP modes 17-9
VTP pruning
overview 17-11
VTP versions 2 and 3
overview 17-9
See also VTP
VTY and Network Assistant 16-12
VVID (voice VLAN ID)
and 802.1X authentication 46-22
configuring 43-3

W

WCCP
- configuration examples 71-10
- configuring on a router 71-2, 71-11
- features 71-4
- restrictions 71-5
- service groups 71-6

web-based authentication
- authentication proxy web pages 48-4
- description 1-43, 46-14, 48-1

web-based authentication, interactions with other features 48-4

Web Cache Communication Protocol
- See WCCP 71-1

web caches
- See cache engines

web cache services
- description 71-4

web caching
- See web cache services
- See also WCCP

web scaling 71-1

weight thresholds in tracked lists 59-5

Wireshark
- activating and deactivating, capture points, conceptual 58-9
- attachment points 58-6
- capture filter 58-7
- capture points 58-6
- core system filter 58-6
- decoding and displaying packets 58-9
- display filter 58-7
- feature interactions 58-10
- filters 58-6
- storing captured packets to a .pcap filter 58-8
- usage examples 58-18

Wireshark, about 58-5

Wireshark, activating and deactivating a capture point 58-13

Wireshark, defining/modifying/deleting a capture point 58-12

Wireshark, displaying information 58-14

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

Y

Y.1731
- default configuration 65-29
- described 65-27
- ETH-AIS
  - Ethernet Alarm Signal function (ETH-AIS) 65-28
- ETH-RDI 65-28
- multicast Ethernet loopback 65-31
- multicast ETH-LB 65-29
- terminology 65-27