INDEX

Numerics

802.1x Accounting
  Overview 13-31

A

AAA down policy, NAC Layer 2 IP validation 1-9
abbreviating commands 2-4
access-class command 37-17
access control entries
  See ACEs
access-denied response, VMPS 17-14
access groups
  Layer 2 37-17
accessing
  clusters, switch 6-11
  member switches 6-11
  switch clusters 6-11
access lists
  See ACLs
access ports
  defined 15-3
  in switch clusters 6-10
accounting
  with IEEE 802.1x 13-13
  with RADIUS 12-16, 12-37
  with TACACS+ 12-6, 12-8, 12-33
ACEs
  and QoS 38-13
  defined 37-2
  Ethernet 37-2
  IP 37-2
ACLs
  ACEs 37-2
  any keyword 37-14
  applying
    time ranges to 37-8, 37-16
    to an interface 37-9, 37-17
    to QoS 38-13
  classifying traffic for QoS 38-36
  comments in 37-8
  defined 37-1, 37-5
  examples of 38-36
  extended IPv4
    creating 37-6, 37-13
    matching criteria 37-5
  hardware and software handling 37-10
  host keyword 37-14
  IP
    creating 37-5
    fragments and QoS guidelines 38-5
    implicit deny 37-7, 37-8, 37-11
    implicit masks 37-11
    matching criteria 37-5
    undefined 37-10
  IPv4
    applying to interfaces 37-9, 37-17
    creating 37-5
    matching criteria 37-5
    named 37-7, 37-15
    numbers 37-5
    terminal lines, setting on 37-9, 37-17
    unsupported features 37-1
  logging messages 37-6
  MAC extended 37-11

matching 37-5, 37-9
named, IPv4 37-7
number per QoS class map 38-5
port 37-2
QoS 38-13, 38-36
resequencing entries 37-7
standard IPv4
creating 37-11
matching criteria 37-5
support for 1-7
support in hardware 37-10
types supported 37-2
unsupported features, IPv4 37-1
active link 24-4, 24-10, 24-11
active links 24-1
active traffic monitoring, IP SLAs 45-1
address aging time for VLANs 7-6
address aliasing 28-2
addresses
dynamic
accelerated aging 20-8
changing the aging time 7-6
default aging 20-8
defined 7-5
learning 7-5
IPv6 42-2
MAC, discovering 7-8
multicast
STP address management 20-8
static
adding and removing 7-6
defined 7-5
address resolution 7-8
Address Resolution Protocol
See ARP
administrative VLAN, REP 23-9
advertisements
CDP 32-1
LLDP 31-2
VTP 17-11, 18-3
age timer, REP 23-8
aggregatable global unicast addresses 42-3
aggregated ports
See EtherChannel
aggregate policers 38-46
aggregate policing 1-10
aging, accelerating 20-8
aging time
accelerated
for STP 20-8
MAC address table 7-13
alarm profiles
creating or modifying 3-8
alarms
displaying 3-9
power supply 3-2
temperature 3-2
allowed-VLAN list 17-12
ARP
defined 1-4, 7-8
table
address resolution 7-8
managing 7-8
attributes, RADIUS
vendor-proprietary 12-17, 12-38
vendor-specific 12-16
attribute-value pairs 13-10, 13-13, 13-19
authentication
local mode with AAA 12-20, 12-39
open1x 13-28
RADIUS
key 12-15
login 12-15, 12-36
TACACS+
defined 12-6
key 12-7, 12-30
login 12-7, 12-31

authentication compatibility with Catalyst 6500 switches 13-7
authentication failed VLAN
See restricted VLAN
authentication manager
CLI commands 13-8
overview 13-6
authoritative time source, described 7-2
authorization
with RADIUS 12-16, 12-37
with TACACS+ 12-6, 12-7, 12-33
authorized ports with IEEE 802.1x 13-9
auto enablement 13-29
automatic discovery
considerations
beyond a noncandidate device 6-8
brand new switches 6-10
connectivity 6-5
different VLANs 6-7
management VLANs 6-8
non-CDP-capable devices 6-7
noncluster-capable devices 6-7
routed ports 6-9
in switch clusters 6-5
See also CDP
automatic QoS
See QoS
auto-MDIX
described 15-10
autonegotiation
duplex mode 1-2
interface configuration guidelines 15-9
mismatches 46-1
autosensing, port speed 1-2
auxiliary VLAN
See voice VLAN
availability, features 1-5

B

BackboneFast
described 22-5
backup interfaces
See Flex Links
backup links 24-1
banners
configuring
login 7-13
message-of-the-day login 7-12
when displayed 7-4
Berkeley r-tools replacement 12-24
binding database
address, DHCP server
See DHCP, Cisco IOS server database
DHCP snooping
See DHCP snooping binding database
bindings
address, Cisco IOS DHCP server 25-6
DHCP snooping database 25-6
IP source guard 27-2
binding table, DHCP snooping
See DHCP snooping binding database
blocking packets 29-4, 29-11
booting
boot loader, function of 4-2
boot process 4-1
specific image 4-17
boot loader
accessing 4-10
described 4-2
environment variables 4-10
prompt 4-10
trap-door mechanism 4-2
BPDU
error-disabled state 22-2
filtering 22-3
RSTP format 21-11

BPDU filtering
described 22-3
support for 1-6
BPDU guard
described 22-2
support for 1-6
bridge protocol data unit
See BPDU
broadcast storm-control command 29-9
broadcast storms 29-1

C

cables, monitoring for unidirectional links 33-1
candidate switch
automatic discovery 6-5
defined 6-2
requirements 6-2
See also command switch, cluster standby group, and member switch
Catalyst 6500 switches
authentication compatibility 13-7
CA trustpoint
configuring 12-23
defined 12-23
CDP
and trusted boundary 38-27
automatic discovery in switch clusters 6-5
configuring 32-2
defined with LLDP 31-1
described 32-1
monitoring 32-3
overview 32-1
support for 1-4
transmission timer and holdtime, setting 32-2
updates 32-2
CGMP
as IGMP snooping learning method 28-7
joining multicast group 28-3
switch support of 1-2
CIP, enabling 10-2
CIP configuration 10-1
CipherSuites 12-24
Cisco 7960 IP Phone 19-1
Cisco Discovery Protocol
See CDP
Cisco Group Management Protocol
See CGMP
Cisco IOS DHCP server
See DHCP, Cisco IOS DHCP server
Cisco IOS File System
See IFS
Cisco IOS IP SLAs 45-2
Cisco Secure ACS
attribute-value pairs for downloadable ACLs 13-19
attribute-value pairs for redirect URL 13-19
Cisco Secure ACS configuration guide 13-48
CiscoWorks 2000 1-3, 36-5
CISP 13-29
CIST regional root
See MSTP
CIST root
See MSTP
civic location 31-3
class maps for QoS
configuring 38-38
described 38-13
displaying 38-56
class of service
See CoS
clearing interfaces 15-19
CLI
abbreviating commands 2-4
command modes 2-1
configuration logging 2-5
described 1-3
editing features
enabling and disabling 2-7

keystroke editing 2-7
wrapped lines 2-9
error messages 2-5
filtering command output 2-10
getting help 2-3
history
changing the buffer size 2-6
described 2-6
disabling 2-7
recalling commands 2-6
managing clusters 6-13
no and default forms of commands 2-4
Client Information Signalling Protocol
See CISP
client mode, VTP 18-3
clock
See system clock
clusters, switch
accessing 6-11
automatic discovery 6-5
benefits 1-2
compatibility 6-4
LRE profile considerations 6-13
managing
through CLI 6-13
through SNMP 6-14
planning considerations
automatic discovery 6-5
CLI 6-13
host names 6-11
IP addresses 6-11
LRE profiles 6-13
passwords 6-12
RADIUS 6-12
SNMP 6-12, 6-14
TACACS+ 6-12
See also candidate switch, command switch, cluster standby group, member switch, and standby command switch
cluster standby group
defined 6-3
requirements 6-2
CNS 1-4
Configuration Engine
configID, deviceID, hostname 5-4
configuration service 5-3
event service 5-3
embedded agents
described 5-5
enabling configuration agent 5-8
enabling event agent 5-7
management functions 1-3
CoA Request Commands 12-12
command-line interface
See CLI
command modes 2-1
commands
abbreviating 2-4
no and default 2-4
commands, setting privilege levels 12-29
command switch
configuration conflicts 46-9
defined 6-3
password privilege levels 6-13
recovery
from lost member connectivity 46-9
requirements 6-1
See also candidate switch, cluster standby group, member switch, and standby command switch
Common Industrial Protocol (CIP) 10-1
community strings
configuring 6-12, 36-6, 36-9
for cluster switches 36-4
in clusters 6-12
overview 36-4
SNMP 6-12
compatibility, feature 29-7
config.text 4-3

configurable leave timer, IGMP 28-5
configuration, initial
defaults 1-11
Express Setup 1-2
configuration changes, logging 35-9
configuration conflicts, recovering from lost member connectivity 46-9
configuration examples, network 1-14
configuration files
archiving A-19
clearing the startup configuration A-19
creating using a text editor A-10
default name 4-3
deleting a stored configuration A-19
described A-9
downloading
preparing A-11, A-13, A-16
reasons for A-9
using FTP A-14
using RCP A-17
using TFTP A-11
guidelines for creating and using A-9
guidelines for replacing and rolling back A-20
invalid combinations when copying A-6
obtaining with DHCP 4-9
password recovery disable considerations 12-3
replacing a running configuration A-19, A-20
rolling back a running configuration A-19, A-20
specifying the filename 4-15
types and location A-10
uploading
preparing A-11, A-13, A-16
reasons for A-9
using FTP A-15
using RCP A-18
using TFTP A-12
configuration guidelines
REP 23-7
configuration logger 35-9
configuration logging 2-5
configuration replacement A-19
configuration rollback A-19
configuration settings, saving 4-17
configure terminal command 15-13
configuring 802.1x user distribution 13-46
configuring small-frame arrival rate 29-10
config-vlan mode 2-2
conflicts, configuration 46-9
connections, secure remote 12-21
consistency checks in VTP Version 2 18-5
console port, connecting to 2-10
control protocol, IP SLAs 45-3
convergence
REP 23-4
corrupted software, recovery steps with Xmodem 46-7
CoS
override priority 19-4
trust priority 19-4
CoS input queue threshold map for QoS 38-22
CoS output queue threshold map for QoS 38-24
CoS-to-DSCP map for QoS 38-47
counters, clearing interface 15-19
CPU utilization, troubleshooting 46-6
crashinfo file 46-5
critical authentication, IEEE 802.1x 13-44
critical VLAN 13-22
cryptographic software image
Kerberos 12-17
SSH 12-1, 12-21
SSL 12-22
customjzeable web pages, web-based authentication 14-6

D

DACL
See downloadable ACL
daylight saving time 7-10
debugging

enabling all system diagnostics 46-12
enabling for a specific feature 46-12
redirecting error message output 46-13
default commands 2-4
default configuration
802.1x 13-30
auto-QoS 39-3
DHCP 25-7
DHCP option 82 25-8
DHCP snooping 25-8
DHCP snooping binding database 25-8
DNS 7-4
EtherChannel 40-10
Ethernet interfaces 15-8
Flex Links 24-5
IGMP filtering 28-12
IGMP snooping 28-6, 44-5
IGMP throttling 28-12
Layer 2 interfaces 15-15
LLDP 31-4
MAC address-table move update 24-5
MSTP 21-13
MVR 28-11
optional spanning-tree configuration 22-9
password and privilege level 12-2
PROFINET 9-4
PTP 8-2
RADIUS 12-10
REP 23-7
RSPAN 30-10
SNMP 36-8
SPAN 30-10
SSL 12-23
standard QoS 38-6
STP 20-11
system message logging 35-5
TACACS+ 12-7
UDLD 33-4
VLANs 17-6
VMPS 17-15
voice VLAN 19-3
VTP 18-9
default gateway 4-14, 4-15
default router preference
See DRP
default web-based authentication configuration
802.1X 14-10
deleting VLANs 17-7, 17-17
denial-of-service attack 29-1
designing your network, examples 1-14
destination addresses
in IPv4 ACLs 37-13
destination-IP address-based forwarding, EtherChannel 40-8
destination-MAC address forwarding, EtherChannel 40-8
detecting indirect link failures, STP 22-5
device discovery protocol 31-1, 32-1
device manager
benefits 1-2
described 1-2, 1-3
in-band management 1-5
DHCP
Cisco IOS server database
default configuration 25-8
described 25-6
enabling
relay agent 25-10
DHCP-based autoconfiguration
client request message exchange 4-5
configuring
client side 4-5
DNS Server 4-8
relay device 4-8
server side 4-7
TFTP server 4-7
lease options
for IP address information 4-7
for receiving the configuration file 4-7

relationship to BOOTP 4-5
relay support 1-4
support for 1-4
DHCP binding database
See DHCP snooping binding database
DHCP binding table
See DHCP snooping binding database
DHCP option 82
circuit ID suboption 25-4
configuration guidelines 25-8
default configuration 25-7
forwarding address, specifying 25-9, 25-10
helper address 25-9
overview 25-3
packet format, suboption
circuit ID 25-4
remote ID 25-4
remote ID suboption 25-4
DHCP server port-based address allocation
default configuration 25-10
described 25-9
enabling 25-13
DHCP server port-based address assignment
support for 1-4
DHCP snooping
accepting untrusted packets form edge switch 25-3, 25-11
binding database
See DHCP snooping binding database
configuration guidelines 25-8
default configuration 25-7
message exchange process 25-4
option 82 data insertion 25-3
trusted interface 25-2
untrusted interface 25-2
untrusted messages 25-2
DHCP snooping binding database
binding file
format 25-7
location 25-6
bindings 25-6
default configuration 25-7, 25-8
described 25-6
displaying
status and statistics 25-14
entry 25-6
DHCP snooping binding table
See DHCP snooping binding database
Differentiated Services architecture, QoS 38-2
Differentiated Services Code Point 38-2
directed unicast requests 1-4
directories
changing A-5
creating and removing A-5
displaying the working A-5
discovery, clusters
See automatic discovery
displaying switch alarms 3-9
DNS
and DHCP-based autoconfiguration 4-8
default configuration 7-4
in IPv6 42-3
overview 7-4
support for 1-4
domain names
DNS 7-4
VTP 18-10
Domain Name System
See DNS
downloadable ACL 13-18, 13-19, 13-48
downloading
configuration files
preparing A-11, A-13, A-16
reasons for A-9
using FTP A-14
using RCP A-17
using TFTP A-11
image files

deleting old image A-26
preparing A-25, A-28, A-32
reasons for A-23
using FTP A-29
using HTTP A-23
using RCP A-33
using TFTP A-25
using the device manager or Network Assistant A-23
DRP
configuring 42-8
described 42-4
IPv6 42-4
DSCP 1-10, 38-2
DSCP input queue threshold map for QoS 38-22
DSCP output queue threshold map for QoS 38-24
DSCP-to-CoS map for QoS 38-48
DSCP-to-DSCP-mutation map for QoS 38-30, 38-49
DSCP transparency 38-27, 38-34
DTP 1-6, 17-9
dual-action detection 40-5
dual IPv4 and IPv6 templates 11-3, 42-5
dual protocol stacks
IPv4 and IPv6 42-5
SDM templates supporting 42-5
dual-purpose uplinks
defined 15-4
LEDs 15-5
link selection 15-5
setting the type 15-15
dynamic access ports
characteristics 17-4
configuring 17-23
defined 15-3
dynamic addresses
See addresses
dynamic ARP inspection
ARP cache poisoning 26-2
ARP requests, described 26-1
ARP spoofing attack 26-2
configuration guidelines 26-5
configuring
ACLs for non-DHCP environments 26-7
in DHCP environments 26-6
log buffer 26-11
rate limit for incoming ARP packets 26-4, 26-9
described 26-1
DHCP snooping binding database 26-2
displaying
ARP ACLs 26-12
configuration and operating state 26-12
trust state and rate limit 26-12
error-disabled state for exceeding rate limit 26-4
function of 26-2
interface trust states 26-3
log buffer
configuring 26-11
logging of dropped packets, described 26-4
man-in-the middle attack, described 26-2
network security issues and interface trust states 26-3
priority of ARP ACLs and DHCP snooping entries 26-4
rate limiting of ARP packets
configuring 26-9
described 26-4
error-disabled state 26-4
validation checks, performing 26-10
dynamic auto trunking mode 17-10
dynamic desirable trunking mode 17-10
Dynamic Host Configuration Protocol
See DHCP-based autoconfiguration
dynamic port VLAN membership
described 17-15
reconfirming 17-16
troubleshooting 17-16
types of connections 17-23
Dynamic Trunking Protocol
See DTP

E

editing features
  enabling and disabling 2-7
  keystrokes used 2-7
  wrapped lines 2-9
ELIN location 31-3
enable password 12-3
enable secret password 12-3
enabling SNMP traps 3-9
encryption, CipherSuite 12-24
encryption for passwords 12-3, 12-27
environment variables, function of 4-11
error-disabled state, BPDU 22-2
error messages during command entry 2-5
EtherChannel
  automatic creation of 40-4, 40-6
  channel groups
    binding physical and logical interfaces 40-3
    numbering of 40-3
  configuration guidelines 40-10
  configuring
    Layer 2 interfaces 40-11
  default configuration 40-10
  forwarding methods 40-8, 40-14
  IEEE 802.3ad, described 40-6
  interaction
    with STP 40-10
    with VLANs 40-11
  LACP
    described 40-6
    hot-standby ports 40-7
    interaction with other features 40-7
    modes 40-6
  load balancing 40-8, 40-14
  logical interfaces, described 40-3
  PAgP
    aggregate-port learners 40-5
    compatibility with Catalyst 1900 40-5
    described 40-4
    interaction with other features 40-6
    interaction with virtual switches 40-5
    learn method and priority configuration 40-5, 40-14
    modes 40-4
    support for 1-2
    with dual-action detection 40-5
  port-channel interfaces
    described 40-3
  port groups 15-4
EtherChannel guard
  described 22-7
Ethernet VLANs
  adding 17-17
  defaults and ranges 17-7
  modifying 17-17
EUI 42-3
examples
  network configuration 1-14
expedite queue for QoS 38-56
Express Setup 1-2
  See also getting started guide
extended crashinfo file 46-5
extended-range VLANs
  configuration guidelines 17-8
  configuring 17-8
  creating with an internal VLAN ID 17-18
extended system ID
  MSTP 21-14
  STP 20-3, 20-11
extended universal identifier
  See EUI
Extensible Authentication Protocol over LAN 13-1

F

fa0 interface 1-5
fallback bridging

connecting interfaces with 15-6
VLAN-bridge STP 20-10
Fast Convergence 24-3
FCS bit error rate alarm
configuring 3-8
defined 3-3
FCS error hysteresis threshold 3-2
features, incompatible 29-7
fiber-optic, detecting unidirectional links 33-1
files
basic crashinfo
description 46-5
location 46-5
copying A-6
crashinfo, description 46-5
deleting A-6
displaying the contents of A-9
extended crashinfo
description 46-5
location 46-5
tar
creating A-7
displaying the contents of A-7
extracting A-8
image file format A-23
file system
displaying available file systems A-1
displaying file information A-4
local file system names A-1
network file system names A-6
setting the default A-3
filtering
non-IP traffic 37-11
show and more command output 2-10
filtering show and more command output 2-10
filters, IP
See ACLs, IP
flash device, number of A-1
flexible authentication ordering
overview 13-27
Flex Link Multicast Fast Convergence 24-3
Flex Links
configuration guidelines 24-6
configuring preferred VLAN 24-12
default configuration 24-5
description 24-1
link load balancing 24-2
VLANs 24-2
flow-based packet classification 1-10
flowcharts
QoS classification 38-12
QoS egress queueing and scheduling 38-23
QoS ingress queueing and scheduling 38-21
QoS policing and marking 38-16
flowcontrol
described 15-9
FTP
configuration files
downloading A-14
overview A-13
preparing the server A-13
uploading A-15
image files
deleting old image A-30
downloading A-29
preparing the server A-28
uploading A-30

G

general query 24-10
Generating IGMP Reports 24-3
get-bulk-request operation 36-4
get-next-request operation 36-4, 36-5
get-request operation 36-4, 36-5
get-response operation 36-4
global configuration mode 2-2
global leave, IGMP 28-7

global status monitoring alarms 3-2
guest VLAN and 802.1x 13-20
GUIs
See device manager and Network Assistant

H

hardware limitations and Layer 3 interfaces 15-12
help, for the command line 2-3
hierarchical policy maps 38-14
configuration guidelines 38-5
configuring 38-29, 38-42
described 38-17
history
changing the buffer size 2-6
described 2-6
disabling 2-7
recalling commands 2-6
history table, level and number of syslog messages 35-9
host names, in clusters 6-11
hosts, limit on dynamic ports 17-16
HP OpenView 1-3
HTTP over SSL
see HTTPS
HTTPS 12-22
configuring 12-42
self-signed certificate 12-23
HTTP secure server 12-22

I

ICMP
IPv6 42-3
time-exceeded messages 46-4
traceroute and 46-4
unreachable messages 37-9
unreachables and ACLs 37-10
ICMP Echo operation
IP SLAs 45-6
ICMP ping
executing 46-9
overview 46-2
ICMPv6 42-3
IEEE 802.1D
See STP
IEEE 802.1p 19-1
IEEE 802.1Q
and trunk ports 15-4
configuration limitations 17-10
native VLAN for untagged traffic 17-12, 17-20
IEEE 802.1s
See MSTP
IEEE 802.1w
See RSTP
IEEE 802.3ad
See EtherChannel
IEEE 802.3x flow control 15-9, 15-16
ifIndex values, SNMP 36-6
IFS 1-5
IGMP
configurable leave timer
described 28-5
flooded multicast traffic
controlling the length of time 28-7
disabling on an interface 28-7
global leave 28-7
query solicitation 28-7
recovering from flood mode 28-7
joining multicast group 28-3
join messages 28-3
leave processing, enabling 44-6, 44-8
leaving multicast group 28-5
queries 28-4
report suppression
described 28-6
supported versions 28-2
support for 1-2

IGMP filtering
configuring 28-13
default configuration 28-12
described 28-12
support for 1-2
IGMP groups
configuring filtering 28-13
setting the maximum number 28-1
IGMP helper 1-2
IGMP Immediate Leave
described 28-5
IGMP profile
applying 28-13
configuration mode 28-13
IGMP snooping
and address aliasing 28-2
default configuration 28-6, 44-5
definition 28-2
enabling and disabling 28-14, 44-6
Immediate Leave 28-5
method 28-6
monitoring 44-9
querier
configuring 28-7, 28-16
supported versions 28-2
support for 1-2
IGMP throttling
configuring 28-13
default configuration 28-12
described 28-12
Immediate Leave, IGMP 28-5
enabling 44-6, 44-8
inaccessible authentication bypass 13-22
support for multiauth ports 13-22
initial configuration
defaults 1-11
Express Setup 1-2
interface
range macros 15-14
interface command 15-6 to 15-13
interface configuration mode 2-3
interfaces
auto-MDIX, configuring 15-10, 15-17
configuration guidelines
duplex and speed 15-9
configuring
procedure 15-13
counters, clearing 15-19
default configuration 15-8
descriptive name, adding 15-17
displaying information about 15-18
flow control 15-9, 15-16
management 1-3
physical, identifying 15-6
range of 15-13
restarting 15-19
shutting down 15-19
speed and duplex, configuring 15-16
supported 15-6
types of 15-1
interfaces range macro command 15-14
interface types 15-6
Internet Protocol version 6
See IPv6
inter-VLAN routing 41-2
Intrusion Detection System
See IDS appliances
inventory management TLV 31-3, 31-5
IP ACLs
for QoS classification 38-13
implicit deny 37-7, 37-11
implicit masks 37-11
named 37-7
undefined 37-10
IP addresses
128-bit 42-2
candidate or member 6-2, 6-11
classes of 41-3

cluster access 6-3
command switch 6-1, 6-11
discovering 7-8
for IP routing 41-3
IPv6 42-2
standby command switch 6-11
See also IP information
ip igmp profile command 28-13
IP information
assigned
manually 4-15
through DHCP-based autoconfiguration 4-4
IP multicast routing
and IGMP snooping 28-2
IP phones
and QoS 19-1
automatic classification and queueing 39-2
ensuring port security with QoS 38-26
trusted boundary for QoS 38-26
IP Port Security for Static Hosts
on a PVLAN host port 27-5
IP precedence 38-2
IP-precedence-to-DSCP map for QoS 38-48
IP protocols
in ACLs 37-13
IP routing
connecting interfaces with 15-6
enabling 41-3
IP Service Level Agreements
See IP SLAs
IP service levels, analyzing 45-1
IP SLAs
benefits 45-2
Control Protocol 45-3
definition 45-1
ICMP echo operation 45-6
measuring network performance 45-3
operation 45-3
responder
described 45-3
response time 45-4
scheduling 45-4
SNMP support 45-2
supported metrics 45-2
threshold monitoring 45-5
UDP jitter operation 45-5
IP source guard
and 802.1x 27-4
and DHCP snooping 27-2
and EtherChannels 27-3
and port security 27-3
and private VLANs 27-3
and routed ports 27-3
and TCAM entries 27-4
and trunk interfaces 27-3
and VRF 27-4
binding configuration
automatic 27-2
manual 27-2
binding table 27-2
configuration guidelines 27-3
described 27-1
filtering
source IP address 27-2
source IP and MAC address 27-2
source IP address filtering 27-2
source IP and MAC address filtering 27-2
IP traceroute
executing 46-10
overview 46-4
IP unicast routing
assigning IP addresses to Layer 3 interfaces 41-4
configuring static routes 41-4
enabling 41-3
inter-VLAN 41-2
IP addressing
classes 41-3
configuring 41-3

steps to configure 41-3
subnet mask 41-3
with SVIs 41-3
IPv4 ACLs
applying to interfaces 37-9, 37-17
extended, creating 37-6, 37-13
named 37-7, 37-15
standard, creating 37-11
IPv4 and IPv6
dual protocol stacks 42-4
IPv6
addresses 42-2
address formats 42-2
applications 42-4
assigning address 42-7
autoconfiguration 42-4
default router preference (DRP) 42-4
defined 42-1
forwarding 42-7
ICMP 42-3
neighbor discovery 42-3
SDM templates 11-3, 44-1
Stateless Autoconfiguration 42-4
supported features 42-2
understanding static routes 42-5

J

join messages, IGMP 28-3

K

KDC
described 12-17
See also Kerberos
Kerberos
authenticating to
boundary switch 12-19
KDC 12-19
network services 12-20
configuring 12-20
credentials 12-17
cryptographic software image 12-17
described 12-17
KDC 12-17
operation 12-19
realm 12-18
server 12-19
support for 1-9
terms 12-18
TGT 12-19
tickets 12-17
key distribution center
See KDC

L

LACP
See EtherChannel
Layer 2 frames, classification with CoS 38-2
Layer 2 interfaces, default configuration 15-15
Layer 2 traceroute
and ARP 46-3
and CDP 46-3
broadcast traffic 46-3
described 46-3
IP addresses and subnets 46-3
MAC addresses and VLANs 46-3
multicast traffic 46-3
multiple devices on a port 46-4
unicast traffic 46-3
usage guidelines 46-3
Layer 3 interfaces
assigning IP addresses to 41-4
changing from Layer 2 mode 41-4
Layer 3 packets, classification methods 38-2
LDAP 5-3

Leaking IGMP Reports 24-4
LEDs, switch
See hardware installation guide
lightweight directory access protocol
See LDAP
line configuration mode 2-3
Link Aggregation Control Protocol
See EtherChannel
link failure, detecting unidirectional 21-7
link fault alarm 3-3
link integrity, verifying with REP 23-4
link local unicast addresses 42-3
link redundancy
See Flex Links
links, unidirectional 33-1
link-state tracking
configuring 43-4
described 43-1
LLDP
configuring
characteristics 31-5
default configuration 31-4
enabling 31-5
monitoring and maintaining 31-8, 31-9
supported TLVs 31-2
switch stack considerations 31-2
transmission timer and holdtime, setting 31-5
LLDP-MED
configuring
TLVs 31-6
monitoring and maintaining 31-8, 31-9
overview 31-2
supported TLVs 31-2
local SPAN 30-2
location TLV 31-3, 31-5
logging messages, ACL 37-6
login authentication
with RADIUS 12-15, 12-36
with TACACS+ 12-7, 12-31
login banners 7-4
loop guard
described 22-8
support for 1-6
LRE profiles, considerations in switch clusters 6-13

M

MAB
See MAC authentication bypass
MAB aging timer 1-7
MAB inactivity timer
default setting 13-31
range 13-34
MAC/PHY configuration status TLV 31-2
MAC addresses
aging time 7-6
and VLAN association 7-5
building the address table 7-5
discovering 7-8
dynamic
learning 7-5
in ACLs 37-11
static
allowing 7-8
characteristics of 7-6
MAC address learning 1-4
MAC address notification, support for 1-11
MAC address-table move update
configuration guidelines 24-6
configuring 24-8
default configuration 24-5
description 24-4
MAC address-to-VLAN mapping 17-14
MAC authentication bypass 13-33
overview 13-14
See MAB
MAC extended access lists
applying to Layer 2 interfaces 37-11

creating 37-11
defined 37-11
for QoS classification 38-10
magic packet 13-24
manageability features 1-4
management access
in-band
browser session 1-5
CLI session 1-5
device manager 1-5
SNMP 1-5
out-of-band console port connection 1-5
management address TLV 31-2
management options
CLI 2-1
CNS 5-2
overview 1-3
management VLAN
considerations in switch clusters 6-8
discovery through different management VLANs 6-8
manual preemption, REP, configuring 23-12
mapping tables for QoS
configuring
CoS-to-DSCP 38-47
DSCP 38-47
DSCP-to-CoS 38-48
DSCP-to-DSCP-mutation 38-30, 38-49
IP-precedence-to-DSCP 38-48
policed-DSCP 38-48
described 38-18
marking
action with aggregate policers 38-46
described 38-4, 38-14
matching, IPv4 ACLs 37-5
maximum number of allowed devices, port-based authentication 13-34
MDA
configuration guidelines 13-10 to 13-11
described 1-8, 13-10
exceptions with authentication process 13-4
membership mode, VLAN port 17-3
member switch
automatic discovery 6-5
defined 6-3
managing 6-13
passwords 6-11
recovering from lost connectivity 46-9
requirements 6-2
See also candidate switch, cluster standby group, and standby command switch
messages, to users through banners 7-4
MIBs
overview 36-2
SNMP interaction with 36-5
mirroring traffic for analysis 30-2
mismatches, autonegotiation 46-1
monitoring
alarms 3-9
cables for unidirectional links 33-1
CDP 32-3
features 1-11
IGMP
snooping 44-9
multicast router interfaces 28-20, 44-9
network traffic for analysis with probe 30-2
port
blocking 29-16
protection 29-16
PTP 8-3, 8-4
SFP status 46-13
speed and duplex mode 15-16
traffic flowing among switches 34-1
VTP 18-14
mrouter Port 24-3
mrouter port 24-10
MSTP
boundary ports
configuration guidelines 21-14

described 21-5
BPDU filtering
described 22-3
BPDU guard
described 22-2
CIST, described 21-3
CIST regional root 21-3
CIST root 21-4
configuration guidelines 21-13
configuring
link type for rapid convergence 21-15
MST region 21-16
neighbor type 21-15
path cost 21-15
port priority 21-15
root switch 21-14, 21-17
secondary root switch 21-15
CST
defined 21-3
operations between regions 21-3
default configuration 21-13
enabling the mode 21-16
EtherChannel guard
described 22-7
extended system ID
effects on root switch 21-14
effects on secondary root switch 21-15
unexpected behavior 21-14
IEEE 802.1s
implementation 21-6
port role naming change 21-6
terminology 21-4
instances supported 20-9
interface state, blocking to forwarding 22-1
interoperability and compatibility among modes 20-10
interoperability with IEEE 802.1D
described 21-8
restarting migration process 21-16
IST
defined 21-2
master 21-3
operations within a region 21-3
loop guard
described 22-8
mapping VLANs to MST instance 21-16
MST region
CIST 21-3
configuring 21-16
described 21-2
hop-count mechanism 21-5
IST 21-2
supported spanning-tree instances 21-2
optional features supported 1-6
overview 21-2
Port Fast
described 22-1
preventing root switch selection 22-7
root guard
described 22-7
root switch
configuring 21-14
effects of extended system ID 21-14
unexpected behavior 21-14
shutdown Port Fast-enabled port 22-2
multiauth
support for inaccessible authentication bypass 13-22
multiauth mode
See multiple-authentication mode
multicast groups
Immediate Leave 28-5
joining 28-3
leaving 28-5
static joins 44-7
multicast router interfaces, monitoring 28-20, 44-9
multicast router ports, adding 28-14, 44-6
multicast storm 29-1
multicast storm-control command 29-9

multicast television application 28-9
multicast VLAN 28-8
Multicast VLAN Registration
See MVR
multidomain authentication
See MDA
multiple authentication 13-11
multiple authentication mode
configuring 13-38
MVR
and address aliasing 28-11
and IGMPv3 28-11
default configuration 28-11
described 28-8
example application 28-9
modes 28-17
multicast television application 28-9
setting global parameters 28-16

N

NAC
AAA down policy 1-9
critical authentication 13-22, 13-44
IEEE 802.1x authentication using a RADIUS server 13-46
IEEE 802.1x validation using RADIUS server 13-46
inaccessible authentication bypass 1-9, 13-44
Layer 2 IEEE 802.1x validation 1-8, 13-27, 13-46
Layer 2 IP validation 1-9
named IPv4 ACLs 37-7
NameSpace Mapper
See NSM
native VLAN
configuring 17-12, 17-20
default 17-12
NEAT
configuring 13-47
overview 13-28
neighbor discovery, IPv6 42-3
neighbor offset numbers, REP 23-5
Network Admission Control
NAC
Network Assistant
benefits 1-2
described 1-3
upgrading a switch A-23
network configuration examples
increasing network performance 1-14
providing network services 1-14
network design
performance 1-14
services 1-14
Network Edge Access Topology
See NEAT
network management
CDP 32-1
RMON 34-1
SNMP 36-1
network performance, measuring with IP SLAs 45-3
network policy TLV 31-2, 31-5
Network Time Protocol
See NTP
no commands 2-4
nonhierarchical policy maps
configuration guidelines 38-5
described 38-15
non-IP traffic filtering 37-11
nontrunking mode 17-10
normal-range VLANs 17-4
configuration guidelines 17-6
configuring 17-4
no switchport command 15-3
NSM 5-4
NTP
associations
defined 7-2
overview 7-2

stratum 7-2
support for 1-4
time
services 7-2
synchronizing 7-2

O

off mode, VTP 18-3
open1x
configuring 13-50
open1x authentication
overview 13-28
Open DeviceNet Vendors Association (ODVA) 10-1
optimizing system resources 11-1
options, management 1-3
out-of-profile markdown 1-10

P

packet modification, with QoS 38-25
PAgP
See EtherChannel
passwords
default configuration 12-2
disabling recovery of 12-3, 12-27
encrypting 12-3, 12-27
for security 1-7
in clusters 6-12
overview 12-2
recovery of 46-8
setting
enable 12-26
enable secret 12-3, 12-27
Telnet 12-28
with usernames 12-4
VTP domain 18-10
path cost
MSTP 21-15
STP 20-13, 20-16
performance, network design 1-14
performance features 1-2
persistent self-signed certificate 12-23
per-user ACLs and Filter-Ids 13-7
per-VLAN spanning-tree plus
See PVST+
physical ports 15-2
PIM-DVMRP, as snooping method 28-7
ping
character output description 46-10
executing 46-9
overview 46-2
policed-DSCP map for QoS 38-48
policers
configuring
for each matched traffic class 38-28
for more than one traffic class 38-46
described 38-4
displaying 38-57
number of 38-6
types of 38-15
policing
described 38-4
hierarchical
See hierarchical policy maps
token-bucket algorithm 38-15
policy maps for QoS
characteristics of 38-28
described 38-13
displaying 38-57
hierarchical 38-14
hierarchical on SVIs
configuration guidelines 38-5
configuring 38-29, 38-42
described 38-17
nonhierarchical on physical ports
configuration guidelines 38-5

described 38-15
port ACLs
defined 37-2
types of 37-2
Port Aggregation Protocol
See EtherChannel
port-based authentication
accounting 13-13
authentication server
defined 13-2, 14-2
RADIUS server 13-2
client, defined 13-2, 14-2
configuring
guest VLAN 13-42
host mode 13-38
inaccessible authentication bypass 13-44
RADIUS server parameters on the switch 13-4, 13-36, 14-10
restricted VLAN 13-43
default configuration 13-30, 14-10
described 13-1
device roles 13-2, 14-2
downloadable ACLs and redirect URLs
overview 13-18 to 13-19
EAPOL-start frame 13-4
EAP-request/identity frame 13-4
EAP-response/identity frame 13-4
enabling
802.1X authentication 14-10, 14-12
encapsulation 13-2
flexible authentication ordering
overview 13-27
guest VLAN
configuration guidelines 13-21, 13-22
described 13-20
host mode 13-9
inaccessible authentication bypass
configuring 13-44
described 13-22
guidelines 13-33
initiation and message exchange 13-4
magic packet 13-24
maximum number of allowed devices per port 13-34
method lists 13-34
multiple authentication 13-11
per-user ACLs
AAA authorization 13-34
configuration tasks 13-17
described 13-17
RADIUS server attributes 13-17
ports
authorization state and dot1x port-control command 13-9
authorized and unauthorized 13-9
voice VLAN 13-23
port security
described 13-24
readiness check
configuring 13-14
described 13-14
resetting to default values 13-51
switch
as proxy 13-2, 14-3
RADIUS client 13-2
switch supplicant
configuring 13-47
overview 13-28
user distribution
guidelines 13-26
overview 13-26
VLAN assignment
AAA authorization 13-34
characteristics 13-15
configuration tasks 13-16
described 13-15
voice aware 802.1x security
configuring 13-16
described 13-16

voice VLAN
described 13-23
PVID 13-23
VVID 13-23
wake-on-LAN, described 13-24
with ACLs and RADIUS Filter-Id attribute 13-29
port-based authentication configuration process 13-34
port-based authentication methods, supported 13-6
port blocking 1-2, 29-4, 29-11
port-channel
See EtherChannel
port description TLV 31-2
Port Fast
described 22-1
mode, spanning tree 17-15
support for 1-6
port membership modes, VLAN 17-3
port not forwarding alarm 3-3
port not operating alarm 3-3
port priority
MSTP 21-15
STP 20-12, 20-16
ports
access 15-3
blocking 29-4, 29-11
dual-purpose uplink 15-4
dynamic access 17-4
protected 29-3
REP 23-6
routed 15-3
secure 29-4
static-access 17-3, 17-7, 17-17
switch 15-2
trunks 17-3, 17-9
VLAN assignments 17-7, 17-17
port security
aging 29-8, 29-15
and QoS trusted boundary 38-26, 38-34
described 29-4
displaying 29-16
on trunk ports 29-13
sticky learning 29-5
violations 29-5
port-shutdown response, VMPS 17-14
port status monitoring alarms
FCS bit error rate alarm 3-3
link fault alarm 3-3
port not forwarding alarm 3-3
port not operating alarm 3-3
port VLAN ID TLV 31-2
power management TLV 31-2, 31-5
preempt delay time, REP 23-5
preemption, default configuration 24-5
preemption delay, default configuration 24-5
preferential treatment of traffic
See QoS
preventing unauthorized access 12-2
primary edge port, REP 23-4
primary links 24-2
priority
overriding CoS 19-4
trusting CoS 19-4
private VLAN edge ports
See protected ports
privileged EXEC mode 2-2
privilege levels
changing the default for lines 12-29
command switch 6-13
exiting 12-30
logging into 12-30
mapping on member switches 6-13
overview 12-2, 12-4
setting a command with 12-29
PROFINET
configuring 9-4
default configuration 9-4
protected ports 1-7, 29-3
protocol storm protection 29-8

proxy reports 24-3
pruning, VTP
enabling
in VTP domain 18-13
on a port 17-19
examples 18-8
overview 18-7
pruning-eligible list
changing 17-19
for VTP pruning 18-7
PTP
configuring 8-3
default configuration 8-2
displaying configuration 8-3, 8-4
PVST+
described 20-9
IEEE 802.1Q trunking interoperability 20-10
instances supported 20-9

Q

QoS
and MQC commands 38-2, 39-2
auto-QoS
categorizing traffic 39-3
disabling 39-8
displaying generated commands 39-8
effects on running configuration 39-7
egress queue defaults 39-3
enabling for VoIP 39-8
ingress queue defaults 39-3
list of generated commands 39-4
basic model 38-4
classification
class maps, described 38-13
defined 38-4
DSCP transparency, described 38-27, 38-34
flowchart 38-12
forwarding treatment 38-3
in frames and packets 38-3
IP ACLs, described 38-11, 38-13
MAC ACLs, described 38-10, 38-13
options for IP traffic 38-10
options for non-IP traffic 38-10
policy maps, described 38-13
trust DSCP, described 38-10
trusted CoS, described 38-10
trust IP precedence, described 38-10
class maps
configuring 38-38
displaying 38-56
configuring
aggregate policers 38-46
default port CoS value 38-33
DSCP maps 38-47
DSCP transparency 38-27, 38-34
DSCP trust states bordering another domain 38-27, 38-35
egress queue characteristics 38-31, 38-52
ingress queue characteristics 38-30, 38-49
IP standard ACLs 38-36
policy maps, hierarchical 38-29, 38-42
port trust states within the domain 38-26, 38-33
trusted boundary 38-26, 38-34
default auto configuration 39-3
default standard configuration 38-6
displaying statistics 38-57
DSCP transparency 38-27, 38-34
egress queues
allocating buffer space 38-31, 38-52
buffer allocation scheme, described 38-23
configuring shaped weights for SRR 38-54
configuring shared weights for SRR 38-55
described 38-4
flowchart 38-23
mapping DSCP or CoS values 38-53
scheduling, described 38-4
setting WTD thresholds 38-31, 38-52

WTD, described 38-24
enabling globally 38-32
flowcharts
classification 38-12
egress queueing and scheduling 38-23
ingress queueing and scheduling 38-21
policing and marking 38-16
implicit deny 38-13
ingress queues
allocating bandwidth 38-51
allocating buffer space 38-50
buffer and bandwidth allocation, described 38-22
configuring shared weights for SRR 38-51
configuring the priority queue 38-30, 38-51
described 38-4
displaying the threshold map 38-57
flowchart 38-21
mapping DSCP or CoS values 38-49
priority queue, described 38-22
scheduling, described 38-4
setting WTD thresholds 38-49
WTD, described 38-22
IP phones
automatic classification and queueing 39-2
detection and trusted settings 38-26, 39-2
limiting bandwidth on egress interface 38-56
mapping tables
CoS-to-DSCP 38-47
displaying 38-57
DSCP-to-CoS 38-48
DSCP-to-DSCP-mutation 38-30, 38-49
IP-precedence-to-DSCP 38-48
policed-DSCP 38-48
types of 38-18
marked-down actions 38-41, 38-44
marking, described 38-4, 38-14
packet modification 38-25
policers
configuring 38-41, 38-44
described 38-14
displaying 38-57
number of 38-6
types of 38-15
policies, attaching to an interface 38-14
policing
described 38-4, 38-14
token bucket algorithm 38-15
policy maps
characteristics of 38-28
displaying 38-57
hierarchical 38-14
hierarchical on SVIs 38-29
nonhierarchical on physical ports 38-28
QoS label, defined 38-4
queues
configuring egress characteristics 38-31, 38-52
configuring ingress characteristics 38-30, 38-49
high priority (expedite) 38-25, 38-56
location of 38-19
SRR, described 38-20
WTD, described 38-19
rewrites 38-25
support for 1-10
trust states
bordering another domain 38-27, 38-35
described 38-10
trusted device 38-26, 38-34
within the domain 38-26, 38-33
quality of service
See QoS
queries, IGMP 28-4
query solicitation, IGMP 28-7

R

RADIUS
attributes
vendor-proprietary 12-17, 12-38

vendor-specific 12-16
configuring
accounting 12-16, 12-37
authentication 12-15, 12-36
authorization 12-16, 12-37
communication, global 12-15, 12-37
communication, per-server 12-14, 12-15
multiple UDP ports 12-14
default configuration 12-10
defining AAA server groups 12-15, 12-35
identifying the server 12-14
in clusters 6-12
limiting the services to the user 12-16
method list, defined 12-15
operation of 12-9
overview 12-8
suggested network environments 12-8
support for 1-9
tracking services accessed by user 12-16, 12-37
RADIUS Change of Authorization 12-10
range
macro 15-14
rapid convergence 21-9
rapid per-VLAN spanning-tree plus
See rapid PVST+
rapid PVST+
described 20-9
IEEE 802.1Q trunking interoperability 20-10
instances supported 20-9
Rapid Spanning Tree Protocol
See RSTP
rcommand command 6-13
RCP
configuration files
downloading A-17
overview A-16
preparing the server A-16
uploading A-18
image files
deleting old image A-34
downloading A-33
preparing the server A-32
uploading A-34
readiness check
port-based authentication
configuring 13-14
described 13-14
reconfirmation interval, VMPS, changing 17-16
redirect URL 13-18, 13-19, 13-48
redundancy
EtherChannel 40-2
STP
backbone 20-7
path cost 17-13
port priority 17-13
reloading software 4-11
Remote Authentication Dial-In User Service
See RADIUS
Remote Copy Protocol
See RCP
Remote SPAN
See RSPAN
remote SPAN 30-2
REP
administrative VLAN 23-9
age timer 23-8
and STP 23-6
configuration guidelines 23-7
convergence 23-4
default configuration 23-7
manual preemption, configuring 23-12
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 23-2
characteristics 23-3
SNMP traps, configuring 23-12
supported interfaces 23-2
triggering VLAN load balancing 23-6
verifying link integrity 23-4
VLAN blocking 23-14
VLAN load balancing 23-4
report suppression, IGMP
described 28-6
resequencing ACL entries 37-7
resetting a UDLD-shutdown interface 33-5
Resilient Ethernet Protocol
See REP
responder, IP SLAs
described 45-3
response time, measuring with IP SLAs 45-4
restricted VLAN
configuring 13-43
described 13-21
using with IEEE 802.1x 13-21
restricting access
overview 12-2
passwords and privilege levels 12-2
RADIUS 12-8
TACACS+ 12-5
RFC
1112, IP multicast and IGMP 28-2
1157, SNMPv1 36-2
1166, IP addresses 41-3
1305, NTP 7-2
1757, RMON 34-2
1901, SNMPv2C 36-2
1902 to 1907, SNMPv2 36-2
2236, IP multicast and IGMP 28-2
2273-2275, SNMPv3 36-2
RFC 5176 Compliance 12-10
RMON
enabling alarms and events 34-3
groups supported 34-2
overview 34-1
statistics
collecting group Ethernet 34-4
collecting group history 34-4
support for 1-11
root guard
described 22-7
support for 1-6
root switch
MSTP 21-14, 21-17
STP 20-11, 20-15
routed ports
defined 15-3
in switch clusters 6-9
IP addresses on 15-12
RSPAN
characteristics 30-7
configuration guidelines 30-9
default configuration 30-10
defined 30-2
destination ports 30-6
monitored ports 30-5
monitoring ports 30-6
overview 1-11, 30-1
received traffic 30-4
sessions
defined 30-3
source ports 30-5
transmitted traffic 30-4
VLAN-based 30-6
RSTP
active topology 21-8
BPDU
format 21-11
processing 21-12
designated port, defined 21-8
designated switch, defined 21-8
interoperability with IEEE 802.1D

described 21-8
restarting migration process 21-16
topology changes 21-12
overview 21-8
port roles
described 21-8
synchronized 21-10
proposal-agreement handshake process 21-9
rapid convergence
described 21-9
edge ports and Port Fast 21-9
point-to-point links 21-9, 21-15
root ports 21-9
root port, defined 21-8
See also MSTP
running configuration
replacing A-19, A-20
rolling back A-19, A-20
running configuration, saving 4-17

S

scheduled reloads 4-11
scheduling, IP SLAs operations 45-4
SCP
and SSH 12-25
SD flash memory card A-2
SDM
templates
number of 11-2
SDM template
configuring 11-4
dual IPv4 and IPv6 11-3
types of 11-2
secondary edge port, REP 23-4
Secure Copy Protocol
Secure Digital flash memory card
See SD flash memory card
secure HTTP client
configuring 12-44
secure MAC addresses
maximum number of 29-5
types of 29-4
secure ports, configuring 29-4
secure remote connections 12-21
Secure Shell
See SSH
Secure Socket Layer
See SSL
security, port 29-4
security features 1-7
See SCP
sequence numbers in log messages 35-8
server mode, VTP 18-3
service-provider network, MSTP and RSTP 21-1
set-request operation 36-5
setting the FCS error hysteresis threshold 3-8
severity levels, defining in system messages 35-8
SFPs
monitoring status of 46-13
security and identification 46-2
status, displaying 46-13
shaped round robin
See SRR
show access-lists hw-summary command 37-10
show and more command output, filtering 2-10
show cdp traffic command 32-3
show cluster members command 6-13
show forward command 46-14
show interfaces command 15-16
show interfaces switchport 24-9
show lldp traffic command 31-9
show platform forward command 46-14
shutdown command on interfaces 15-19
Simple Network Management Protocol
See SNMP
small-frame arrival rate, configuring 29-10
Smartports macros

applying global parameter values 16-3
configuration guidelines 16-2
default configuration 16-1
tracing 16-2
SNAP 32-1
SNMP
accessing MIB variables with 36-5
agent
described 36-4
disabling 36-8
and IP SLAs 45-2
authentication level 36-11
community strings
configuring 36-6, 36-9
for cluster switches 36-4
overview 36-4
configuration examples 36-15
default configuration 36-8
engine ID 36-1
groups 36-1, 36-10
host 36-1
ifIndex values 36-6
in-band management 1-5
in clusters 6-12
informs
and trap keyword 36-6, 36-12
described 36-5
differences from traps 36-5
limiting access by TFTP servers 36-15
limiting system log messages to NMS 35-9
manager functions 1-3, 36-4
managing clusters with 6-14
notifications 36-5
overview 36-2, 36-5
security levels 36-3
setting CPU threshold notification 36-14
system contact and location 36-14
trap manager, configuring 36-12
traps
described 36-4, 36-5
differences from informs 36-5
enabling 36-6, 36-12
enabling MAC address notification 7-14, 7-15
overview 36-2, 36-5
types of 36-7
users 36-1, 36-10
versions supported 36-2
SNMP and Syslog Over IPv6 42-5
SNMP traps
REP 23-12
SNMPv1 36-3
SNMPv2C 36-3
SNMPv3 36-3
snooping, IGMP 28-2
software images
location in flash A-23
recovery procedures 46-7
tar file format, described A-23
See also downloading and uploading
source addresses
in IPv4 ACLs 37-13
source-and-destination-IP address based forwarding, EtherChannel 40-9
source-and-destination MAC address forwarding, EtherChannel 40-8
source-IP address based forwarding, EtherChannel 40-8
source-MAC address forwarding, EtherChannel 40-8
SPAN
configuration guidelines 30-9
default configuration 30-10
destination ports 30-6
monitored ports 30-5
monitoring ports 30-6
overview 1-11, 30-1
ports, restrictions 29-7
received traffic 30-4
sessions
defined 30-3

source ports 30-5
transmitted traffic 30-4
VLAN-based 30-6
spanning tree and native VLANs 17-10
Spanning Tree Protocol
See STP
SRR
configuring
shaped weights on egress queues 38-54
shared weights on egress queues 38-55
shared weights on ingress queues 38-51
described 38-20
shaped mode 38-20
shared mode 38-20
support for 1-10, 1-11
SSH
cryptographic software image 12-1, 12-21
described 1-5, 12-21
encryption methods 12-21
user authentication methods, supported 12-21
SSL
configuring a secure HTTP client 12-44
configuring a secure HTTP server 12-42
cryptographic software image 12-22
described 12-22
standby command switch
configuring
defined 6-3
requirements 6-2
See also cluster standby group and HSRP
standby group, cluster
See cluster standby group and HSRP
standby links 24-2
startup configuration
booting
specific image 4-17
clearing A-19
configuration file
specifying the filename 4-15
static access ports
assigning to VLAN 17-7, 17-17
defined 15-3, 17-3
static addresses
See addresses
static MAC addressing 1-7
static routes
configuring 41-4
understanding 42-5
static VLAN membership 17-2
statistics
interface 15-18
QoS ingress and egress 38-57
RMON group Ethernet 34-4
RMON group history 34-4
VTP 18-14
sticky learning 29-5
storm control
configuring 29-3, 29-9
displaying 29-16
support for 1-2
thresholds 29-1
STP
accelerating root port selection 22-4
and REP 23-6
BackboneFast
described 22-5
BPDU filtering
described 22-3
BPDU guard
described 22-2
BPDU message exchange 20-2
configuration guidelines 20-13
configuring
path cost 20-13, 20-16
port priority 20-12, 20-16
root switch 20-11, 20-15
secondary root switch 20-12, 20-16
spanning-tree mode 20-14

switch priority 20-17
default configuration 20-11
default optional feature configuration 22-9
designated port, defined 20-3
designated switch, defined 20-3
detecting indirect link failures 22-5
disabling 20-11
EtherChannel guard
described 22-7
extended system ID
effects on root switch 20-11
effects on the secondary root switch 20-12
overview 20-3
unexpected behavior 20-12
features supported 1-6
IEEE 802.1D and bridge ID 20-3
IEEE 802.1D and multicast addresses 20-8
IEEE 802.1t and VLAN identifier 20-4
inferior BPDU 20-3
instances supported 20-9
interface state, blocking to forwarding 22-1
interface states
blocking 20-5
disabled 20-6
forwarding 20-5, 20-6
learning 20-6
listening 20-6
overview 20-4
interoperability and compatibility among modes 20-10
limitations with IEEE 802.1Q trunks 20-10
load sharing
overview 17-12
using path costs 17-13
using port priorities 17-13
loop guard
described 22-8
modes supported 20-9
multicast addresses, effect of 20-8
optional features supported 1-6
path costs 17-13
Port Fast
described 22-1
preventing root switch selection 22-7
protocols supported 20-9
redundant connectivity 20-7
root guard
described 22-7
root port, defined 20-3
root switch
configuring 20-12
effects of extended system ID 20-3, 20-11
election 20-3
unexpected behavior 20-12
shutdown Port Fast-enabled port 22-2
superior BPDU 20-3
UplinkFast
described 22-3
VLAN-bridge 20-10
stratum, NTP 7-2
subnet mask 41-3
success response, VMPS 17-14
summer time 7-10
SunNet Manager 1-3
supported port-based authentication methods 13-6
SVI autostate exclude
configuring 15-10
SVIs
and IP unicast routing 41-3
connecting VLANs 15-5
routing between VLANs 17-2
switch 42-2
switch boot process 4-1
switch console port 1-5
Switch Database Management
See SDM
Switched Port Analyzer
See SPAN

switched ports 15-2
switch information assignment 4-4
switchport backup interface 24-4, 24-10
switchport block multicast command 29-11
switchport block unicast command 29-11
switchport command 15-8
switchport protected command 29-11
switch priority
  STP 20-17
switch software features 1-1
system capabilities TLV 31-2
system clock
  configuring
    daylight saving time 7-10
    manually 7-9
    summer time 7-10
    time zones 7-9
  overview 7-1
  See also NTP
system description TLV 31-2
system message logging
  default configuration 35-5
  defining error message severity levels 35-8
  disabling 35-5
  facility keywords, described 35-4
  level keywords, described 35-3
  limiting messages 35-9
  message format 35-2
  overview 35-1
  sequence numbers, enabling and disabling 35-8
  setting the display destination device 35-6
  synchronizing log messages 35-2, 35-7
  syslog facility 1-11
  time stamps, enabling and disabling 35-8
  UNIX syslog servers
    configuring the daemon 35-4
    configuring the logging facility 35-10
    facilities supported 35-4
system name
  manual configuration 7-11
  See also DNS
system name TLV 31-2
system prompt, default setting 7-5
system resources, optimizing 11-1

T

TACACS+
  accounting, defined 12-6
  authentication, defined 12-6
  authorization, defined 12-6
  configuring
    accounting 12-8, 12-33
    authentication key 12-7, 12-30
    authorization 12-7, 12-33
    login authentication 12-7, 12-31
  default configuration 12-7
  identifying the server 12-7, 12-30
  in clusters 6-12
  limiting the services to the user 12-7
  operation of 12-6
  overview 12-5
  support for 1-9
  tracking services accessed by user 12-8, 12-33
tar files
  creating A-7
  displaying the contents of A-7
  extracting A-8
  image file format A-23
TDR 1-11
Telnet
  accessing management interfaces 2-10
  number of connections 1-5
  setting a password 12-28
temporary self-signed certificate 12-23
Terminal Access Controller Access Control System Plus
  See TACACS+
terminal lines, setting a password 12-28

TFTP
configuration files
downloading A-11
preparing the server A-11
uploading A-12
configuration files in base directory 4-8
configuring for autoconfiguration 4-7
image files
deleting A-26
downloading A-25
preparing the server A-25
uploading A-27
limiting access by servers 36-15
TFTP server 1-4
threshold, traffic level 29-2
threshold monitoring, IP SLAs 45-5
time
See NTP and system clock
Time Domain Reflector
See TDR
time-range command 37-8
time ranges in ACLs 37-8, 37-16
time stamps in log messages 35-8
time zones 7-9
TLVs
defined 31-2
LLDP 31-2
LLDP-MED 31-2
Token Ring VLANs
support for 17-5
VTP support 18-5
ToS 1-10
traceroute, Layer 2
and ARP 46-3
and CDP 46-3
broadcast traffic 46-3
described 46-3
IP addresses and subnets 46-3
MAC addresses and VLANs 46-3
multicast traffic 46-3
multiple devices on a port 46-4
unicast traffic 46-3
usage guidelines 46-3
traceroute command 46-10
See also IP traceroute
traffic
blocking flooded 29-11
fragmented 37-3
unfragmented 37-3
traffic policing 1-10
traffic suppression 29-1
transparent mode, VTP 18-3
trap-door mechanism 4-2
traps
configuring MAC address notification 7-14, 7-15
configuring managers 36-6, 36-12
defined 36-4
enabling 7-14, 7-15, 36-6, 36-12
notification types 36-7
overview 36-2, 36-5
triggering alarm options
configurable relay 3-3
methods 3-3
SNMP traps 3-3
syslog messages 3-4
troubleshooting
CPU utilization 46-6
displaying crash information 46-5
setting packet forwarding 46-14
SFP security and identification 46-2
show forward command 46-14
with CiscoWorks 36-5
with ping 46-2
with system message logging 35-1
with traceroute 46-4
trunk failover
See link-state tracking
trunking encapsulation 1-6

trunk ports
defined 15-4, 17-3
trunks
allowed-VLAN list 17-12, 17-19
load sharing
setting STP path costs 17-13
using STP port priorities 17-13
native VLAN for untagged traffic 17-12, 17-20
parallel 17-13
pruning-eligible list 17-19
to non-DTP device 17-9
trusted boundary for QoS 38-26, 38-34
trusted port states
between QoS domains 38-27, 38-35
classification options 38-10
ensuring port security for IP phones 38-26, 38-34
support for 1-10
within a QoS domain 38-26, 38-33
trustpoints, CA 12-23
twisted-pair Ethernet, detecting unidirectional links 33-1
type of service
See ToS

U

UDLD
default configuration 33-4
echoing detection mechanism 33-3
enabling
globally 33-4
per interface 33-5
link-detection mechanism 33-1
neighbor database 33-2
overview 33-1
resetting an interface 33-5
support for 1-5
UDP jitter operation, IP SLAs 45-5
unauthorized ports with IEEE 802.1x 13-9
unicast MAC address filtering 1-4
and adding static addresses 7-7
and broadcast MAC addresses 7-7
and CPU packets 7-7
and multicast addresses 7-7
and router MAC addresses 7-7
configuration guidelines 7-7
described 7-7
unicast storm 29-1
unicast storm control command 29-9
UNIX syslog servers
daemon configuration 35-4
facilities supported 35-4
message logging configuration 35-10
unrecognized Type-Length-Value (TLV) support 18-5
upgrading software images
See downloading
UplinkFast
described 22-3
uploading
configuration files
preparing A-11, A-13, A-16
reasons for A-9
using FTP A-15
using RCP A-18
using TFTP A-12
image files
preparing A-25, A-28, A-32
reasons for A-23
using FTP A-30
using RCP A-34
using TFTP A-27
user EXEC mode 2-2
username-based authentication 12-4

V

version-dependent transparent mode 18-5
virtual switches and PAgP 40-5
vlan.dat file 17-4

VLAN 1, disabling on a trunk port 17-12
VLAN 1 minimization 17-12
vlan-assignment response, VMPS 17-14
VLAN blocking, REP 23-14
VLAN configuration
at bootup 17-5
saving 17-5
VLAN configuration mode 2-2
VLAN database
and startup configuration file 17-5
VLAN configuration saved in 17-5
VLANs saved in 17-4
VLAN filtering and SPAN 30-6
vlan global configuration command 17-5
VLAN ID, discovering 7-8
VLAN load balancing
REP 23-4
VLAN load balancing, triggering 23-6
VLAN load balancing on flex links 24-2
configuration guidelines 24-6
VLAN management domain 18-2
VLAN membership
modes 17-3
VLAN Query Protocol
See VQP
VLANs
adding 17-17
adding to VLAN database 17-7
aging dynamic addresses 20-8
allowed on trunk 17-12, 17-19
and spanning-tree instances 17-3, 17-6, 17-8
configuration guidelines, extended-range VLANs 17-8
configuration guidelines, normal-range VLANs 17-6
configuring 17-1
configuring IDs 17-8
connecting through SVIs 15-5
default configuration 17-6
deleting 17-7, 17-17
described 15-2, 17-1
extended-range 17-8
features 1-6
illustrated 17-2
internal 17-9
modifying 17-17
multicast 28-8
native, configuring 17-12, 17-20
normal-range 17-4
number supported 1-6
parameters 17-5
port membership modes 17-3
static-access ports 17-7, 17-17
STP and IEEE 802.1Q trunks 20-10
supported 17-2
Token Ring 17-5
traffic between 17-2
VLAN-bridge STP 20-10
VLAN Trunking Protocol
See VTP
VLAN trunks 17-9
VMPS
configuration example 17-24
configuration guidelines 17-15
default configuration 17-15
description 17-14
dynamic port membership
described 17-15
reconfirming 17-16
troubleshooting 17-16
entering server address 17-22
mapping MAC addresses to VLANs 17-14
reconfirmation interval, changing 17-16
voice aware 802.1x security
port-based authentication
configuring 13-16
described 13-16
voice-over-IP 19-1
voice VLAN

Cisco 7960 phone, port connections 19-1
configuration guidelines 19-3
configuring IP phones for data traffic
override CoS of incoming frame 19-4
trust CoS priority of incoming frame 19-4
configuring ports for voice traffic in
802.1p priority tagged frames 19-5
802.1Q frames 19-5
connecting to an IP phone 19-4
default configuration 19-3
described 19-1
displaying 19-6
IP phone data traffic, described 19-3
IP phone voice traffic, described 19-2
VQP 1-6, 17-14
VTP
adding a client to a domain 18-10, 18-13
advertisements 17-11, 18-4
and extended-range VLANs 17-2, 18-2
and normal-range VLANs 17-2, 18-2
configuration
guidelines 18-9
saving 18-9
configuration requirements 18-1, 20-1
configuration revision number
guideline 18-10, 18-13
resetting 18-14
consistency checks 18-5
default configuration 18-9
described 18-2
domain names 18-10
domains 18-2
modes
client 18-3
off 18-3
server 18-3
transparent 18-3
monitoring 18-14
passwords 18-10
pruning
enabling 18-13
examples 18-8
overview 18-7
support for 1-6
pruning-eligible list, changing 17-19
statistics 18-14
support for 1-6
Token Ring support 18-5
transparent mode, configuring 18-4
using 18-2
Version
enabling 18-12
version, guidelines 18-6
Version 1 18-5
Version 2
configuration guidelines 18-6
overview 18-5
Version 3
overview 18-5

W

web authentication 13-14
described 1-7
web-based authentication
customizeable web pages 14-6
description 14-2
web-based authentication, interactions with other features 14-8
weighted tail drop
See WTD
wired location service
configuring 31-7
displaying 31-8, 31-9
location TLV 31-3
understanding 31-3
WTD
described 38-19

setting thresholds
egress queue-sets 38-31, 38-52
ingress queues 38-49
support for 1-10, 1-11

X

Xmodem protocol 46-7