Numerics

10/100 autonegotiation feature, forced 4-7
802.10 SAID (default) 10-4
802.1Q
  trunks 14-6
tunneling
    compatibility with other features 19-5
defaults 19-4
described 19-2
tunnel ports with other features 19-6
802.1Q VLANs
  encapsulation 12-3
trunk restrictions 12-5
802.1s
  See MST
802.1w
  See MST
802.1X
  See port-based authentication
802.1X authentication
  for guest VLANs 31-6
  RADIUS accounting 31-7
  with port security 31-6
  with VLAN assignment 31-5
  with voice VLAN ports 31-10
802.3ad
  See LACP

A
  abbreviating commands 2-5
  access control entries
    See ACEs
  access list filtering, SPAN enhancement 39-13
  access ports
    and Layer 2 protocol tunneling 19-9
    configuring 12-8
  access VLANs 12-6
  accounting
    configuring for 802.1X 31-16
  ACEs
    ACLs 35-2
    Ethernet 35-2
    IP 35-2
    Layer 4 operation restrictions 35-8
  ACLs
    ACEs 35-2
    and SPAN 39-5
    and TCAM programming 35-6
    applying on routed packets 35-21
    applying on switched packets 35-20
    compatibility on the same switch 35-3
    configuring with VLAN maps 35-20
    CPU impact 35-9
    hardware and software support 35-5
    IP, matching criteria for port ACLs 35-4
    MAC extended 35-11
    matching criteria for router ACLs 35-3
    port
      and voice VLAN 35-4
      defined 35-2
limitations 35-4
processing 35-9
types supported 35-2
acronyms, list of A-1
active queue management 29-13
addresses
  See MAC addresses
adjacency tables
description 24-2
displaying statistics 24-9
advertisements, VTP
  See VTP advertisements
alarms
  major 7-2
  minor 7-2
asymmetrical links, and 802.1Q tunneling 19-4
audience xxi
authentication
  See also port-based authentication
authentication server
  defined 31-3
  RADIUS server 31-3
authorized and unauthorized ports 31-4
authorized ports with 802.1X 31-4
autoconfiguration 3-2
automatic QoS
  See QoS
autonegotiation feature
  forced 10/100Mbps 4-7
Auto-QoS
  configuring 29-16
auto-sync command 6-8

B

BackboneFast
  adding a switch (figure) 15-2
  and MST 16-2
  configuring 15-15

link failure (figure) 15-7, 15-8
not supported MST 16-2
understanding 15-6
  See also STP
BGP 1-8
  routing session with multi-VRF CE 28-6
  blocking packets 37-1
  blocking state (STP)
    RSTP comparisons (table) 16-4
  boot bootldr command 3-24
  boot command 3-21
  boot fields
    See configuration register boot fields
  boot system command 3-19, 3-24
  boot system flash command 3-21
Border Gateway Protocol
  See BGP
boundary ports
description 16-6
BPDU Guard
  and MST 16-2
  configuring 15-12
  overview 15-4
BPDUs
  and media speed 14-2
  pseudobridges and 16-5
  what they contain 14-3
bridge ID
  See STP bridge ID
bridge priority (STP) 14-16
bridge protocol data units
  See BPDUs
broadcast storm control
disabling 38-4
BSR
  configuration example 25-21
burst rate 29-44
burst size 29-27
candidate switch
defined  9-12
requirements  9-12
See also command switch and member switch
cautions for passwords
encrypting  3-16
TACACS+  3-15
CDP
and trusted boundary  29-25
configuration  20-2
displaying configuration  20-3
enabling on interfaces  20-3
Layer 2 protocol tunneling  19-7
maintaining  20-3
monitoring  20-3
overview  1-2, 20-1
cdp enable command  20-3
CEF
adjacency tables  24-2
configuring load balancing  24-7
displaying statistics  24-8
enabling  24-6
hardware switching  24-4
load balancing  24-6
overview  24-1
software switching  24-4
CGMP
overview  18-1
channel-group group command  17-7, 17-10
Cisco Discovery Protocol
See CDP
Cisco Express Forwarding
See CEF
Cisco Group Management Protocol
See CGMP
Cisco IOS NSF-awareness support  6-2
Cisco IP Phones
configuring  30-2
Cisco IP phones
sound quality  30-1
CIST
description  16-2
class-map command  29-28
class of service
See CoS
clear cdp counters command  20-4
clear cdp table command  20-3
clear counters command  4-14
clearing
IP multicast table entries  25-20
clear ip flow stats command  40-8
CLI
accessing  2-1
backing out one level  2-5
getting commands  2-5
history substitution  2-3
managing clusters  9-13
modes  2-5
monitoring environments  39-1
ROM monitor  2-6
software basics  2-4
clients
in 802.1X authentication  31-2
clustering switches
command switch characteristics  9-11, 9-12
and VTY  9-12
managing
through CLI  9-13
overview  9-11
planning considerations
CLI  9-13
command-line processing  2-3
command modes  2-5
commands
listing  2-5
command switch
requirements 9-11
common and internal spanning tree
  See CIST
common spanning tree
  See CST
community ports
description 36-1
community VLANs
  and SPAN features 36-4
  configure as a PVLAN 36-5
description 36-1
config-register command 3-22
config terminal command 3-9
configuration files
  obtaining with DHCP 3-6
  saving 3-10
configuration register
  boot fields
    listing value 3-22
    modifying 3-21
    changing settings 3-21 to 3-22
    configuring 3-19
    settings at startup 3-20
configure terminal command 3-22, 4-2
console configuration mode 2-5
console port
  disconnecting user sessions 5-5
  monitoring user sessions 5-4
copy running-config startup-config command 3-10
copy system:running-config nvram:startup-config command 3-24
CoS
  configuring port value 29-41
definition 29-3
figure 29-2
  overriding on Cisco IP Phones 30-3
priority 30-3
CoS-to-DSCP maps 29-46
counters
  clearing MFIB 25-20
  clearing on interfaces 4-14
  CPU port sniffing 39-10
  CST
    description 16-5
    IST and 16-2
    MST and 16-2
customer edge devices 28-2

D
default configuration
  802.1X 31-12
  auto-QoS 29-16
  IGMP filtering 18-17
  Layer 2 protocol tunneling 19-9
  multi-VRF CE 28-3
  SPAN and RSPAN 39-6
default gateway
  configuring 3-11
  verifying configuration 3-11
default ports
  and support for 802.1X authentication 31-13
description command 4-9
detecting unidirectional links 21-1
DHCP-based autoconfiguration
  client request message exchange 3-3
  configuring
    client side 3-2
    DNS 3-5
    relay device 3-5
    server-side 3-3
    TFTP server 3-4
  example 3-7
  lease options
    for IP address information 3-4
    for receiving the configuration file 3-4
  overview 3-2
  relationship to BOOTP 3-2
DHCP snooping
configuring 33-3
default configuration 33-3
displaying binding tables 33-10
displaying configuration 33-10
enabling 33-4
enabling on private VLAN 33-5
enabling the database agent 33-6
monitoring 33-9, 33-13, 33-14
overview 33-1
Snooping database agent 33-2
DHCP Snooping Database Agent
adding to the database (example) 33-9
enabling (example) 33-6
overview 33-2
reading from a TFTP file (example) 33-8
Differentiated Services Code Point values
See DSCP values
DiffServ architecture, QoS 29-2
disabled state
RSTP comparisons (table) 16-4
disabling
broadcast storm control 38-4
disconnect command 5-5
DNS
and DHCP-based autoconfiguration 3-5
documentation
organization xxi
related xxiii
double-tagged packets
802.1Q tunneling 19-2
Layer 2 protocol tunneling 19-9
drop threshold for Layer 2 protocol packets 19-9
DSCP maps 29-45
DSCP-to-CoS maps
configuring 29-47
DSCP values
configuring maps 29-45
configuring port value 29-42
definition 29-3
IP precedence 29-2
mapping markdown 29-23
mapping to transmit queues 29-43
DTP
VLAN trunks and 12-3
duplex command 4-8
duplex mode
configuring interface 4-7
Dynamic Host Configuration Protocol snooping
See DHCP snooping
dynamic port VLAN membership
limit on hosts 11-9
reconfirming 11-7
troubleshooting 11-9
Dynamic Trunking Protocol
See DTP

E
EAP frame
request/identity 31-3
response/identity 31-3
EAP frames
changing retransmission time 31-20
exchanging (figure) 31-4
setting retransmission number 31-21
EAPOL frames
802.1X authentication and 31-2
OTP authentication, example (figure) 31-4
start 31-3
edge ports
description 16-7
EGP
overview 1-8
EIGRP
overview 1-8
Embedded CiscoView
displaying information 9-16
installing and configuring  9-14
overview  9-13
enable command  3-9, 3-21
enable mode  2-5
encapsulation types  12-3
Enhanced Interior Gateway Routing Protocol
See EIGRP
environmental monitoring
LED indications  7-2
SNMP traps  7-2
supervisor engine  7-2
switching modules  7-2
using CLI commands  7-1
EtherChannel
channel-group group command  17-7, 17-10
configuration guidelines  17-5
configuring  17-6 to 17-14
configuring Layer 2  17-9
configuring Layer 3  17-6
interface port-channel command  17-7
lacp system-priority
command example  17-12
modes  17-3
overview  17-1
PAgP
   Understanding  17-3
physical interface configuration  17-7
port-channel interfaces  17-2
port-channel load-balance command  17-12
ports, 802.1X authentication not supported in  31-13
removing  17-14
removing interfaces  17-13
explicit host tracking
enabling  18-8
extended range VLANs
   See VLANs
Extensible Authentication Protocol over LAN  31-2
Exterior Gateway Protocol
   See EGP

FastDrop
   clearing entries  25-20
   displaying entries  25-19
   overview  25-10
FIB
   description  24-2
   See also MFIB
   filtering
   in a VLAN  35-12
   non-IP traffic  35-11
   flags  25-11
Flash memory
   configuring router to boot from  3-24
   loading system images from  3-23
   security precautions  3-23
   flooded traffic, blocking  37-2
   forward-delay time (STP)
   configuring  14-18
   forwarding information base
   See FIB

gateway
   See default gateway
global configuration mode  2-5
Guest-VLANs
   configure with 802.1X  31-17, 31-18

hardware and software ACL support  35-5
hardware switching  24-5
hello time (STP)
   configuring  14-17
history
   CLI  2-3
hop counts
  configuring MST bridges  16-7
host
  configuring host statically  18-8
  limit on dynamic port  11-9
Hot Standby Routing Protocol
  See HSRP
HSRP
  description  1-6
hw-module module num power command  7-15
ICMP
  enabling  5-10
  ping  5-5
  running IP traceroute  5-7
  time exceeded messages  5-7
IDS
  using with SPAN and RSPAN  39-2
IEEE 802.1s
  See MST
IEEE 802.1w
  See MST
IEEE 802.3ad
  See LACP
IGMP
  description  25-3
  enabling  25-13
  explicit host tracking  18-3, 18-8
  immediate-leave processing  18-3
  overview  18-1
IGMP filtering
  configuring  18-17
  default configuration  18-17
  described  18-16
  monitoring  18-20
IGMP groups
  setting the maximum number  18-19
IGMP profile
  applying  18-18
  configuration mode  18-17
  configuring  18-17
IGMP snooping
  configuration guidelines  18-4
  enabling  18-5
  IP multicast and  25-4
  monitoring  18-11
  overview  18-1
IGRP
  description  1-8
  immediate-leave processing
    enabling  18-7
  IGMP
    See fast-leave processing
  ingress packets, SPAN enhancement  39-12
  inline power
    configuring on Cisco IP phones  30-4
  Intelligent Power Management  8-5
  interface command  3-9, 4-1
  interface port-channel command  17-7
  interface range command  4-4
  interface range macro command  4-5
  interfaces
    adding descriptive name  4-9
    clearing counters  4-14
    configuring  4-2
    configuring ranges  4-4
    displaying information about  4-13
  Layer 2 modes  12-4
  maintaining  4-13
  monitoring  4-13
  naming  4-9
  numbers  4-2
  overview  4-1
  restarting  4-14
  See also Layer 2 interfaces
Interior Gateway Routing Protocol
See IGRP
Internet Control Message Protocol
See ICMP
Internet Group Management Protocol
See IGMP
Inter-Switch Link encapsulation
See ISL encapsulation
Intrusion Detection System
See IDS

IP
  configuring default gateway 3-11
  configuring static routes 3-11
displaying statistics 24-8
flow switching cache 40-8
IP addresses
  candidate or member 9-12
  command switch 9-12
  See also IP information
ip cef command 24-6
ip flow-aggregation cache destination-prefix command 40-10
ip flow-aggregation cache prefix command 40-10
ip flow-aggregation cache source-prefix command 40-10
ip flow-export command 40-8
ip icmp rate-limit unreachable command 5-11
ip igmp profile command 18-17
ip igmp snooping tcn flood command 18-10
ip igmp snooping tcn flood query count command 18-10
ip igmp snooping tcn query solicit command 18-11
IP information
  assigned
    through DHCP-based autoconfiguration 3-2
ip load-sharing per-destination command 24-7
ip local policy route-map command 26-5
ip mask-reply command 5-12
IP multicast
  clearing table entries 25-20
  configuring 25-12
  default configuration 25-13
displaying PIM information 25-15
displaying the routing table information 25-16
enabling 25-13
enabling dense-mode PIM 25-14
enabling sparse-mode 25-14
features not supported 25-12
hardware forwarding 25-8
IGMP snooping and 18-4, 25-4
monitoring 25-15
overview 25-1
routin protocols 25-2
software forwarding 25-8
See also Auto-RP; IGMP; PIM; RP; RPF
ip multicast-routing command 25-13
IP phones
  automatic classification and queueing 29-16
  configuring voice ports 30-2
  See Cisco IP Phones 30-1
  trusted boundary for QoS 29-24
ip pim command 25-14
ip pim dense-mode command 25-14
ip pim sparse-dense-mode command 25-15
ip policy route-map command 26-4
ip redirects command 5-11
ip route-cache flow command 40-7
IP routing tables
  deleting entries 25-20
IP Source Guard
  configuring 33-11
  configuring on private VLANs 33-12
displaying 33-13, 33-14
overview 33-10
IP statistics
  displaying 24-8
IP traceroute
  executing 5-7
overview 5-7
IP unicast
displaying statistics 24-8
ip unreachable command 5-10
IPX
    redistribution of route information with EIGRP 1-8
ISL
    encapsulation 12-3
    trunking with 802.1Q tunneling 19-4
isolated ports
    description 36-1
isolated VLANs
    description 36-1
IST
    description 16-2
    master 16-7
    MST regions and 16-2

J
jumbo frames
    and ethernet ports 4-11
    configuring MTU sizes for 4-12
    ports and linecards that support 4-10
    VLAN interfaces 4-11

K
keyboard shortcuts 2-3

L
l2protocol-tunnel command 19-11
labels
    definition 29-3
LACP
    system ID 17-4
Layer 2 access ports 12-8
Layer 2 frames
    classification with CoS 29-2
Layer 2 interfaces
    assigning VLANs 10-8
    configuring 12-5
    configuring as PVLAN host ports 36-8
    configuring as PVLAN promiscuous ports 36-7
    configuring as PVLAN trunk ports 36-9
    defaults 12-5
    disabling configuration 12-9
    modes 12-4
    show interfaces command 12-7
Layer 2 interface type
    resetting 36-12
    setting 36-12
Layer 2 protocol tunneling
    configuring 19-9
    default configuration 19-9
    defined 19-7
    guidelines 19-10
Layer 2 switching
    overview 12-1
Layer 2 Traceroute
    and ARP 5-9
    and CDP 5-8
    described 5-8
    host-to-host paths 5-8
    IP addresses and subnets 5-9
    MAC addresses and VLANs 5-9
    multicast traffic 5-9
    multiple devices on a port 5-9
    unicast traffic 1-3, 5-8
    usage guidelines 5-8
Layer 2 trunks
    configuring 12-6
    overview 12-3
Layer 3 packets
    classification methods 29-2
Layer 4 port operations
    configuration guidelines 35-8
    restrictions 35-8
LEDs
description (table) 7-2
listening state (STP)RSTP comparisons (table) 16-4
load balancing
configuring for CEF 24-7
configuring for EtherChannel 17-12
overview 17-5, 24-6
per-destination 24-7
login timer
changing 5-4
logoutwarning command 5-4
loop guard
and MST 16-2
configuring 15-9
overview 15-2

M
MAC addresses
allocating 14-5
building tables 12-2
convert dynamic to sticky secure 32-2
displaying 5-3
displaying in DHCP snooping binding table 33-10
in ACLs 35-11
sticky 32-2
sticky secure, adding 32-2
MAC extended access lists 35-11
macros
See SmartPort macros
main-cpu command 6-8
mapping
DSCP markdown values 29-23
DSCP values to transmit queues 29-43
mapping tables
configuring DSCP 29-45
described 29-13
mask destination command 40-10
mask source command 40-10
match ip address command 26-3
maximum aging time (STP)
configuring 14-18
member switch
defined 9-11
managing 9-13
requirements 9-12
metro tags 19-2
MFIB
CEF 25-5
displaying 25-18
overview 25-11
modules
checking status 5-1
powering down 7-15
monitoring
802.1Q tunneling 19-12
ACL information 35-28
IGMP filters 18-20
IGMP snooping 18-11
Layer 2 protocol tunneling 19-12
multi-VRF CE 28-11
tunneling 19-12
VLAN filters 35-19
VLAN maps 35-19
M-record 16-2
MST
and multiple spanning trees 1-4, 16-2
boundary ports 16-6
BPDUs 16-2
configuration parameters 16-5
configuring 16-9
displaying configurations 16-13
edge ports 16-7
enabling 16-9
hop count 16-7
instances
configuring parameters 16-12
description 16-2
number supported 16-5
interoperability with PVST+ 16-2
link type 16-7
master 16-7
message age 16-7
regions 16-5, 16-6
restrictions 16-8
to-SST interoperability 16-4

MSTP
M-record 16-2
M-tree 16-2
M-tree 16-2
MTU size
configuring 4-12
default 10-4
multicast
See IP multicast
multicast packets
blocking 37-2
multicast routers
displaying routing tables 25-16
flood suppression 18-9
Multicast Storm Control
overview 38-6
suppression on WS-X4014 38-7
suppression on WS-X4016 38-6
multiple forwarding paths 1-4, 16-2

Multiple Spanning Tree
See MST
multiple VPN routing/forwarding
See multi-VRF CE

multi-VRF CE
components 28-3
configuration example 28-7
default configuration 28-3
defined 28-1
displaying 28-11
monitoring 28-11
network components 28-3

packet-forwarding process 28-3

native VLAN
and 802.1Q tunneling 19-4
specifying 12-6

NetFlow
aggregation
minimum mask, default value 40-10
destination-prefix aggregation
configuration (example) 40-15
minimum mask, configuring 40-10
prefix aggregation
configuration (example) 40-13
minimum mask, configuring 40-10
source-prefix aggregation
minimum mask, configuring 40-10
switching
configuration (example) 40-11
configuring 40-7
exporting cache entries 40-8
statistics 40-8

NetFlow statistics
caveats on supervisor 40-6
configuring collection 40-6
implementing collection 40-6
overview of collection 40-1

Network Assistant
and VTY 9-12
configure
display configuration 9-9
enable communication with switch 9-4
enable inter-cluster communication 9-7
connect to a device 9-10
default configuration 9-3
installation requirements 9-2
installing 9-3
launch 9-10
overview of CLI commands 9-4
software and hardware requirements 9-2
understanding 9-2
network fault tolerance 1-4, 16-2
network management configuring 20-1
Next Hop Resolution Protocol See NHRP
NFFC/NFFC II
IGMP snooping and 18-4
NHRP support 1-8
non-IP traffic filtering 35-11
non-RPF traffic description 25-9
in redundant configurations (figure) 25-10
nonvolatile random-access memory See NVRAM
normal-range VLANs See VLANs
NSF-awareness support 6-2
NVRAM saving settings 3-10

P
packets modifying 29-15
software processed and QoS 29-15
packet type filtering overview 39-14
SPAN enhancement 39-14
SPAN enhancement
PAgP
understanding 17-3
passwords configuring enable password 3-14
configuring enable secret password 3-14
encrypting 3-15
recovering lost enable password 3-18
setting line password 3-14
setting TACACS+ 3-15
PBR (policy-based routing)
configuration (example) 26-5
enabling 26-3
features 26-2
overview 26-1
route maps 26-2
when to use 26-2
per-port and VLAN Access Control List 33-10
Per-VLAN Rapid Spanning Tree 14-6
enabling 14-20
overview 14-6
PE to CE routing, configuring 28-6
PIM configuring dense mode 25-14
configuring sparse mode 25-14
displaying information 25-15
displaying statistics 25-20
enabling sparse-dense mode 25-14, 25-15
overview 25-3
PIM-DM 25-3
PIM-SM 25-3

O
OIR overview 4-13
online insertion and removal See OIR
Open Shortest Path First See OSPF
operating system images See system images
OSPF area concept 1-7
description 1-7
ping
   executing 5-6
   overview 5-5
ping command 5-6, 25-15
PoE 8-7
   configuring power consumption for single device 8-4
   configuring power consumption for switch 8-4
   power consumption for powered devices
      Intelligent Power Management 8-5
         overview 8-3
         supported cabling topology 8-5
         powering down a module 7-15
         power management modes 8-1
         show interface status 8-6
point-to-point
   in 802.1X authentication (figure) 31-2, 31-8
police command 29-32
policed-DSCP map 29-46
policers
   description 29-5
   types of 29-9
policies
   See QoS policies
   policing
      See QoS policing
policy-map command 29-29, 29-31
policy maps
   attaching to interfaces 29-34
   configuring 29-30
port ACLs
   and voice VLAN 35-4
   defined 35-2
   limitations 35-4
Port Aggregation Protocol
   see PAgP
port-based authentication
   802.1X with voice VLAN 31-10
   changing the quiet period 31-19
   client, defined 31-2
   configuration guidelines 31-13
   configure 802.1X accounting 31-16
   configure switch-to-RADIUS server communication 31-15
   configure with Guest-VLANs 31-17, 31-18
   configuring Guest-VLAN 31-15
   configuring manual re-authentication of a client 31-19
   controlling authorization state 31-4
   default configuration 31-12
   described 31-2
   device roles 31-2
   disabling 31-14
   displaying statistics 31-22
   enabling 31-13
   enabling multiple hosts 31-21
   enabling periodic re-authentication 31-18
   encapsulation 31-2
   initiation and message exchange 31-3
   method lists 31-13
   ports not supported 31-4
   resetting to default values 31-22
   setting retransmission number 31-21
   setting retransmission time 31-20
   topologies, supported 31-10
   using with port security 31-6
   with VLAN assignment 31-5
port-based QoS features
   See QoS
   port-channel interfaces
      See also EtherChannel
      creating 17-6
      overview 17-2
   port-channel load-balance
      command 17-12
      command example 17-12
   port-channel load-balance command 17-12
   port cost (STP)
      configuring 14-15
   PortFast
and MST 16-2
BPDU filter, configuring 15-12
configuring or enabling 15-11
overview 15-3
PortFast BPDU filtering
and MST 16-2
enabling 15-12
overview 15-4
port priority
configuring MST instances 16-12
configuring STP 14-13
ports
blocking 37-1
checking status 5-2
community 36-1
dynamic VLAN membership
reconfirming 11-7
forwarding, resuming 37-3
isolated 36-1
PVLAN types 36-1
secure 32-1
See also interfaces
port security
aging 32-6
and QoS trusted boundary 29-24
configuring 32-4
default configuration 32-3
described 32-1
displaying 32-7
RADIUS accounting 31-7
sticky learning 32-2
using with 802.1X 31-6
violations 32-2
with other features 32-3
port states
description 14-5
port trust state
See trust states
power
inline 30-4
power dc input command 7-11
power inline command 8-2
power inline consumption command 8-4
power management
1+1 redundancy mode 7-12
2+1 redundancy mode 7-12
Catalyst 4006 switch 7-12
Catalyst 4500 series 7-4
Catalyst 4500 Series power supplies 7-9
Catalyst 4948 series 7-3
combined mode 7-5
configuring combined mode 7-8
configuring redundant mode 7-7
overview 7-1
redundancy 7-12
redundant mode 7-5
power redundancy
setting on Catalyst 4006 7-14
power redundancy-mode command 7-8
power supplies
fixed 7-4
variable 7-3, 7-4
power supplies required command 7-14
primary VLANs
associating with secondary VLANs 36-6
configuring as a PVLAN 36-5
description 36-1
priority
overriding CoS of incoming frames 30-3
privileged EXEC mode 2-5
privileges
changing default 3-17
configuring levels 3-16
exiting 3-17
logging in 3-17
promiscuous ports
configuring PVLAN 36-7
description 36-1
setting mode 36-12
protocol timers 14-4
provider edge devices 28-2
pruning, VTP
  See VTP pruning
pseudobridges
description 16-5
PVACL 33-10
PVID (port VLAN ID)
  and 802.1X with voice VLAN ports 31-10
PVLANs
  802.1q support 36-5
  configuration guidelines 36-3
  configuring 36-3
  configuring a VLAN 36-5
  configuring promiscuous ports 36-7
  host ports
    configuring a Layer 2 interface 36-8
    setting 36-12
isolated VLANs 36-1
overview 36-1
permitting routing, example 36-11
promiscuous mode
  setting 36-12
setting
  interface mode 36-12

Q

QoS

allocating bandwidth 29-44
and software processed packets 29-15
avto-QoS
  configuration and defaults display 29-19
  configuration guidelines 29-17
  described 29-16
  displaying 29-19
  effects on NVRAM configuration 29-17
  enabling for VoIP 29-18
  basic model 29-5
  burst size 29-27
  classification 29-5 to 29-9
  configuration guidelines 29-24
    auto-QoS 29-17
  configuring
    auto-QoS 29-16
    DSCP maps 29-45
    traffic shaping 29-44
    trusted boundary 29-24
  VLAN-based 29-39
  configuring user based rate limiting 29-35
    hierarchical policers 29-37
  creating policing rules 29-28
  default auto configuration 29-16
  default configuration 29-22
  definitions 29-3
  disabling on interfaces 29-34
  enabling on interfaces 29-34
  flowcharts 29-7, 29-11
IP phones
  automatic classification and queueing 29-16
  detection and trusted settings 29-16, 29-24
  overview 29-1
  packet modification 29-15
  port-based 29-39
  priority 29-14
  traffic shaping 29-14
  transmit rate 29-44
  trust states
    trusted device 29-24
  VLAN-based 29-39
  See also COS; DSCP values; transmit queues
QoS active queue management
  tracking queue length 29-13
QoS labels
  definition 29-3
QoS mapping tables
  CoS-to-DSCP 29-46
DSCP-to-CoS 29-47
policed-DSCP 29-46
types 29-13
QoS marking
description 29-4
QoS policers
burst size 29-27
types of 29-9
QoS policing
definition 29-4
described 29-5, 29-9
QoS policy
attaching to interfaces 29-10
overview of configuration 29-28
QoS transmit queues
allocating bandwidth 29-44
burst 29-14
configuring 29-43
configuring traffic shaping 29-44
mapping DHCP values to 29-43
maximum rate 29-14
overview 29-13
sharing link bandwidth 29-14
Quality of service
See QoS
queueing 29-5, 29-13

See RSTP
rcommand command 9-13
re-authentication of a client
configuring manual 31-19
enabling periodic 31-18
reduced MAC address 14-2
redundancy
configuring 6-8
guidelines and restrictions 6-7
changes made through SNMP 6-8, 6-10
NSF-awareness support 6-2
overview 6-3
redundancy command 6-8
understanding synchronization 6-6
redundancy(RPR)
route processor redundancy 6-4
synchronization 6-6
redundancy(SSO)
route processor redundancy 6-4
synchronization 6-7
related documentation xxiii
reload command 3-21, 3-22
replication
description 25-8
reserved-range VLANs
See VLANs
retransmission number
setting in 802.1X authentication 31-21
retransmission time
changing in 802.1X authentication 31-20
RIP
description 1-7
ROM monitor
boot process and 3-19
CLI 2-6
root bridge
configuring 14-9
selecting in MST 16-2
root guard

R

RADIUS server
configure to-Switch communication 31-15
configuring settings 31-16
parameters on the switch 31-15
range command 4-4
range macros
defining 4-5
ranges of interfaces
configuring 4-4
Rapid Spanning Tree
and MST 16-2
enabling 15-8
overview 15-2
routed packets
   ACLs 35-21
route-map (IP) command 26-3
route maps
   defining 26-3
PBR 26-2
router ACLs
   description 35-2
   using with VLAN maps 35-20
route targets
   VPN 28-3
Routing Information Protocol
   See RIP
RSPAN
   configuration guidelines 39-16
destination ports 39-5
IDS 39-2
monitored ports 39-4
monitoring ports 39-5
received traffic 39-3
sessions
   creating 39-17
   defined 39-3
   limiting source traffic to specific VLANs 39-23
   monitoring VLANs 39-22
   removing source (monitored) ports 39-21
   specifying monitored ports 39-17
source ports 39-4
transmitted traffic 39-4
VLAN-based 39-5
RSTP
compatibility 16-3
description 16-2
port roles 16-3
port states 16-4

S
SAID
   See 802.10 SAID
scheduling 29-13
   defined 29-4
   overview 29-5
secondary root switch 14-12
secondary VLANs
   associating with primary 36-6
   description 36-2
   permitting routing 36-11
secure ports, configuring 32-1
Security Association Identifier
   See 802.10 SAID
servers, VTP
   See VTP servers
service-policy command 29-29
service-policy input command 22-2, 29-34
service-provider networks
   and customer VLANs 19-2
   Layer 2 protocols across 19-7
set default interface command 26-4
set interface command 26-4
set ip default next-hop command 26-4
set ip next-hop command 26-4
show adjacency command 24-9
show boot command 3-24
show catalyst4000 chassis-mac-address command 14-3
show cdp command 20-2, 20-3
show cdp entry command 20-4
show cdp interface command 20-3
show cdp neighbors command 20-4
show cdp traffic command 20-4
show ciscoview package command 9-16
show ciscoview version command 9-16
show cluster members command 9-13
show configuration command 4-9
show debugging command 20-4
show environment command 7-2
show history command 2-4
show interfaces command 4-12, 4-13
show interfaces status command 5-2
show ip cache flow aggregation destination-prefix command 40-11
show ip cache flow aggregation prefix command 40-11
show ip cache flow aggregation source-prefix command 40-11
show ip cache flow command 40-8
show ip cef command 24-8
show ip interface command 25-15
show ip local policy command 26-5
show ip mroute command 25-15
show ip pim interface command 25-15
show l2protocol command 19-11
show mac-address-table address command 5-3
show mac-address-table interface command 5-3
show mls entry command 24-8
show module command 5-1, 14-5
show PoE consumed 8-7
show power command 7-14
show power inline command 8-6
show power inline consumption command 8-4
show power supplies command 7-8
show protocols command 4-13
show running-config command
  adding description for an interface 4-9
  checking your settings 3-9
  displaying ACLs 35-14, 35-16, 35-23, 35-24
show startup-config command 3-10
show users command 5-4
show version command 3-22
shutdown, command 4-14
shutdown threshold for Layer 2 protocol packets 19-9
shutting down interfaces 4-14
single spanning tree
  See SST
slot numbers, description 4-2
SmartPort macros
  configuration guidelines 13-4
  configuring 13-2
  creating and applying 13-4
  default configuration 13-2
  defined 13-1
  displaying 13-8
  tracing 13-4
SNMP
  documentation 1-13
  support 1-13
software
  upgrading 6-12
software configuration register 3-19
software switching
  description 24-5
  interfaces 24-6
  key data structures used 25-7
SPAN
  and ACLs 39-5
  configuration guidelines 39-7
  configuring 39-6 to 39-10
  destination ports 39-5
  IDS 39-2
  monitored port, defined 39-4
  monitoring port, defined 39-5
  received traffic 39-3
  sessions
    defined 39-3
    source ports 39-4
    transmitted traffic 39-4
VLAN-based 39-5
SPAN and RSPAN
  concepts and terminology 39-3
  default configuration 39-6
  displaying status 39-24
  overview 39-1
  session limits 39-6
SPAN destination ports
802.1X authentication not supported 31-13
SPAN enhancements
access list filtering 39-13
configuration example 39-15
CPU port sniffing 39-10
encapsulation configuration 39-12
ingress packets 39-12
packet type filtering 39-14
spanning-tree backbonefast command 15-15
spanning-tree cost command 14-15
spanning-tree guard root command 15-8
spanning-tree portfast bpdu-guard command 15-12
spanning-tree portfast command 15-11
spanning-tree port-priority command 14-13
spanning-tree uplinkfast command 15-14
spanning-tree vlan command 14-9
command example 14-9
spanning-tree vlan command 14-8
spanning-tree vlan cost command 14-15
spanning-tree vlan forward-time command 14-19
spanning-tree vlan hello-time command 14-17
spanning-tree vlan max-age command 14-18
spanning-tree vlan port-priority command 14-13
spanning-tree vlan priority command 14-17
spanning-tree vlan root primary command 14-10
spanning-tree vlan root secondary command 14-12
speed
configuring interface 4-7
speed command 4-7
SST
description 16-2
interoperability 16-4
static routes
configuring 3-11
verifying 3-12
statistics
displaying 802.1X 31-22
displaying PIM 25-20
NetFlow accounting 40-8
sticky learning
configuration file 32-2
defined 32-2
disabling 32-2
enabling 32-2
saving addresses 32-2
sticky MAC addresses
counting 32-4
defined 32-2
Storm Control
disabling 38-4
displaying 38-4
enabling 38-3
hardware-based, implementing 38-2
overview 38-1
STP
bridge ID 14-2
configuring 14-7 to 14-20
creating topology 14-4
defaults 14-6
disabling 14-19
enabling 14-7
enabling extended system ID 14-8
enabling Per-VLAN Rapid Spanning Tree 14-20
forward-delay time 14-18
hello time 14-17
Layer 2 protocol tunneling 19-7
maximum aging time 14-18
overview 14-1, 14-3
per-VLAN rapid spanning tree 14-6
port cost 14-15
port priority 14-13
root bridge 14-9
supervisor engine
accessing the redundant 6-14
configuring 3-8 to 3-13
copying files to standby 6-14
default configuration 3-1
default gateways 3-11
environmental monitoring 7-1
ROM monitor 3-19
startup configuration 3-18
static routes 3-11
synchronizing configurations 6-10
SVIs
and router ACLs 35-3
switched packets
and ACLs 35-20
Switched Port Analyzer
See SPAN
switching, NetFlow
configuration (example) 40-11
configuring 40-7
exporting cache entries 40-8
switchport
show interfaces 4-12
switchport access vlan command 12-6, 12-8
switchport block multicast command 37-2
switchport block unicast command 37-2
switchport mode access command 12-8
switchport mode dot1q-tunnel command 19-6
switchport mode dynamic command 12-6
switchport mode trunk command 12-6
switch ports
See access ports
switchport trunk allowed vlan command 12-6
switchport trunk encapsulation command 12-6
switchport trunk encapsulation dot1q command 12-3
switchport trunk encapsulation isl command 12-3
switchport trunk encapsulation negotiate command 12-3
switchport trunk native vlan command 12-6
switchport trunk pruning vlan command 12-6
switch-to-RADIUS server communication
configuring 31-15
syslog messages 7-2
system
reviewing configuration 3-10
settings at startup 3-20
system images
loading from Flash memory 3-23
modifying boot field 3-20
specifying 3-23
system MTU
802.1Q tunneling 19-5
maximums 19-5

T

TACACS+
setting passwords 3-15
tagged packets
802.1Q 19-3
Layer 2 protocol 19-7
TCAM programming and ACLs 35-6
Telnet
accessing CLI 2-2
disconnecting user sessions 5-5
executing 5-3
monitoring user sessions 5-4
telnet command 5-4
TFTP
configuration files in base directory 3-5
configuring for autoconfiguration 3-5
time exceeded messages 5-7
timer
See login timer
Token Ring
media not supported (note) 10-4, 27-3
TOS
description 29-3
trace command 5-7
trace command
See IP traceroute
See Layer 2 Traceroute
trace route mac command 5-9
traceroute mac ip command 5-9
traffic
  blocking flooded 37-2
traffic control
  using ACLs (figure) 35-4
  using VLAN maps (figure) 35-5
traffic shaping 29-14
translational bridge numbers (defaults) 10-4
transmit queues
  See QoS transmit queues
transmit rate 29-44
troubleshooting
  with traceroute 5-7
trunk ports
  802.1X authentication not supported on 31-13
  configuring PVLAN 36-9 to 36-11
trunks
  802.1Q restrictions 12-5
  configuring 12-6
  configuring access VLANs 12-6
  configuring allowed VLANs 12-6
  default interface configuration 12-6
  different VTP domains 12-3
  enabling to non-DTP device 12-4
  encapsulation 12-3
  specifying native VLAN 12-6
  understanding 12-3
trusted boundary for QoS 29-24
trust states
  configuring 29-40
tunneling
  defined 19-1
  Layer 2 protocol 19-7
tunnel ports
  802.1Q, configuring 19-6
  described 19-2
  incompatibilities with other features 19-5
type of service
  See TOS

U

UDLD
  default configuration 21-2
  disabling 21-3
  enabling 21-3
  overview 21-1, 34-1
unauthorized ports with 802.1X 31-4
unicast
  See IP unicast
unicast flood blocking
  configuring 37-1
unicast traffic
  blocking 37-2
unidirectional ethernet
  enabling 22-2
  example of setting 22-2
  overview 22-1
UniDirectional Link Detection Protocol
  See UDLD
UplinkFast
  and MST 16-2
  enabling 15-14
  MST and 16-3
  overview 15-5
user EXEC mode 2-5
user sessions
  disconnecting 5-5
  monitoring 5-4

V

VACLs
  Layer 4 port operations 35-7
virtual LANs
  See VLANs
Virtual Private Network
  See VPN
VLAN ACLs
See VLAN maps

VLAN Management Policy Server
See VMPS

VLAN Trunking Protocol
See VTP

VMPS
configuring dynamic access ports on client 11-6
configuring retry interval 11-8
dynamic port membership
reconfirming 11-7
reconfirming assignments 11-7
reconfirming membership interval 11-7
server overview 11-1

VMPS client
administering and monitoring 11-8
configure switch
configure reconfirmation interval 11-7
dynamic ports 11-6
entering IP VMPS address 11-5
reconfirmation interval 11-8
reconfirm VLAM membership 11-7
default configuration 11-4
dynamic VLAN membership overview 11-4
troubleshooting dynamic port VLAN membership 11-9

VMPS server
fall-back VLAN 11-3
illegal VMPS client requests 11-3
overview 11-1
security modes
multiple 11-3
open 11-2
secure 11-3

Voice over IP
configuring 30-1
voice ports
configuring VVID 30-2
voice traffic 8-1, 30-4
voice VLAN ports

VLAN maps
applying 35-16, 35-24
common uses for 35-16
configuration example 35-17
configuration guidelines 35-13
configuring 35-12
creating entries 35-13
defined 35-3
denyng access example 35-18
denying packets 35-14
displaying 35-19
dynamizing 35-18
examples 35-18
order of entries 35-13
permitting packets 35-14
router ACLs and 35-20
using (figure) 35-5

VLANs
allowed on trunk 12-6
configuration guidelines 10-3
configuring 10-4
customer numbering in service-provider networks 19-3
default configuration 10-4
description 1-5
extended range 10-3
IDs (default) 10-4
interface assignment 10-8
limiting source traffic with RSPAN 39-23
monitoring with RSPAN 39-22
name (default) 10-4
normal range 10-3
overview 10-1
reserved range 10-3
See also PVLANs

vlan command 10-6, 10-7
vlan database command 10-7
vlan dot1q tag native command 19-4

VTP

Voice over IP
configuring 30-1
voice ports
configuring VVID 30-2
voice traffic 8-1, 30-4
voice VLAN ports
using 802.1X  31-10

VPN
  configuring routing in  28-5
  forwarding  28-3
  in service provider networks  28-1
  routes  28-2
  routing and forwarding table
    See VRF

VRF
  defining  28-3
  tables  28-1

VTP
  configuration guidelines  27-5
  configuring  27-6 to 27-10
  configuring transparent mode  27-9
  default configuration  27-5
  disabling  27-9
  Layer 2 protocol tunneling  19-7
  monitoring  27-10
  overview  27-1
  See also VTP version 2

VTP advertisements
  description  27-3

VTP clients
  configuring  27-8

VTP domains
  description  27-2

VTP modes  27-2

VTP pruning
  enabling  27-6
  overview  27-3

VTP servers
  configuring  27-7

VTP statistics
  displaying  27-10

VTP version 2
  enabling  27-7
  overview  27-3
  See also VTP

VTY and Network Assistant  9-12

VVID (voice VLAN ID)
  and 802.1X authentication  31-10
  configuring  30-2