



Cisco LAN Switching Configuration Handbook

Second Edition

A complete, concise reference for implementing the most important features of the Cisco Catalyst family of switches

Cisco LAN Switching Configuration Handbook

Steve McQuerry, David Jansen, David Hucaby

Copyright © 2009 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing June 2009

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58705-610-9

ISBN-10: 1-58705-610-0

Warning and Disclaimer

This book is designed to provide information about the configuration of Cisco Catalyst switches. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsoned.com

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Senior Development Editor: Christopher Cleveland

Project Editor: Seth Kerney

Editorial Assistant: Vanessa Evans

Book and Cover Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Tim Wright

Cisco Representative: Eric Ullanderson

Cisco Press Program Manager: Anand Sundaram

Technical Editors: Ron Fuller, Don Johnston

Copy Editor: Apostrophe Editing Services

Proofreader: Language Logistics, LLC



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CQVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Introduction

Of the many sources of information and documentation about Cisco Catalyst switches, few provide a quick and portable solution for networking professionals.

Cisco LAN Switching Configuration Handbook is designed to provide a quick and easy reference guide for all the features that can be configured on Cisco Catalyst switches. In essence, the subject matter from an entire bookshelf of Catalyst software documentation, along with other networking reference material, has been “squashed” into one handy volume that you can take with you.

The idea for this book began as a follow-on to the router configuration book. In larger switched network environments, it is common to see many different Catalyst platforms in use—each might have a different feature set. We have found it difficult to remember the configuration steps and commands when moving from one Catalyst platform to another. Perhaps you have, too.

As with router configuration, the commands for switch configuration went into a notebook of handwritten notes. This notebook began to travel with us into the field as a network consultant and engineer. When you’re on the job and someone requires you to configure a feature that you’re not too familiar with, it’s nice to have your handy reference notebook in your bag! Hopefully, this book will be that handy reference for you as well.

Note This book is based on the most current Cisco Catalyst software releases at press time—IOS switches according to the 12.2 major release. If you use an earlier version of either software, you might find that the configuration commands differ slightly.

Features

This book is meant to be used as a tool in your day-to-day tasks as a network administrator, engineer, consultant, or student. As such, we have avoided presenting a large amount of instructional information or theory on the operation of features or commands. That is better handled in other textbooks that are dedicated to a more limited subject matter.

Instead, the book is divided into chapters that present quick facts, configuration steps, and explanations of configuration options for each Cisco Catalyst switch feature. The chapters are as follows:

- **Chapter 1, “CLI Usage”:** Describes the IOS environment and command-line interface
- **Chapter 2, “Switch Functionality”:** Describes LAN switches and how to implement a switch campus network design
- **Chapter 3, “Supervisor Engine Configuration”:** Explains how to configure switch prompts, IP addresses, passwords, switch modules, file management, and administrative protocols

- **Chapter 4, “Layer 2 Interface Configuration”:** Describes configuration of Ethernet, Fast Ethernet, Gigabit Ethernet, and EtherChannel interfaces
- **Chapter 5, “Layer 3 Interface Configuration”:** Explains how Layer 3 interfaces are used in a switch
- **Chapter 6, “VLANs and Trunking”:** Presents VLAN configuration, private VLANs, trunking, and VTP
- **Chapter 7, “Spanning Tree Protocol (STP)”:** Discusses STP operation, configuration, and tuning
- **Chapter 8, “Configuring High Availability Features”:** Explains how to configure and use Catalyst switch hardware for redundancy using multiple supervisors and hot standby routing protocol (HSRP)
- **Chapter 9, “Multicast”:** Explains how a switch handles multicast traffic and interacts with multicast routers
- **Chapter 10, “Server Load Balancing (SLB)”:** Presents Catalyst 6500 features that streamline access to server and firewall farms
- **Chapter 11, “Controlling Traffic and Switch Access”:** Discusses broadcast suppression, user authentication, port security, and VLAN access lists
- **Chapter 12, “Switch Management”:** Explains how to configure a switch for logging, SNMP and RMON management, port analysis (SPAN), power management, and connectivity testing
- **Chapter 13, “Quality of Service”:** Presents configuration of QoS theory and features in a switched network
- **Chapter 14, “Voice”:** Discusses specialized voice gateway modules, inline power, and QoS features needed to transport voice traffic
- **Appendix A, “Cabling Quick Reference,” and Appendix B, “Well-Known Protocol, Port, and Other Numbers”:** Present a cabling quick reference and a table of well-known ports and addresses

How to Use This Book

All the information in this book has been designed to follow a quick-reference format. If you know what feature or technology you want to use, you can turn right to the section that deals with it. Sections are numbered with a quick-reference index, showing both chapter and section number (5-2, for example, is Chapter 5, section 2). You'll also find shaded index tabs on each page, listing the section number.

Facts About a Feature

Each section in a chapter begins with a bulleted list of quick facts about the feature, technology, or protocol. Refer to these lists to quickly learn or review how the feature works.

Configuration Steps

Each feature that is covered in a section includes the required and optional commands used for common configuration. The difference is that the configuration steps are presented in an outline format. If you follow the outline, you can configure a complex feature or technology. If you find that you don't need a certain feature option, skip over that level in the outline.

Example Configurations

Each section includes an example of how to implement the commands and their options. We tried to present the examples with the commands listed in the order you would actually enter them to follow the outline. Many times, it is more difficult to study and understand a configuration example from an actual switch because the commands are displayed in a predefined order—not in the order you entered them. The examples have also been trimmed down to show only the commands presented in the section (where possible).

Displaying Information About a Feature

Where applicable, each section concludes with a brief summary of the commands you can use to show information about the switch feature. You can use these command summaries as a quick reference when you are debugging or troubleshooting switch operation.

Further Reading

Most chapters conclude with a recommended reading list to help you find more in-depth sources of information for the topics discussed.

Server Load Balancing (SLB)

See the following sections to configure and use these features:

- **10-1: SLB:** Covers the configuration steps needed to provide load balancing of traffic to one or more server farms
- **10-2: SLB Firewall Load Balancing:** Discusses the configuration steps necessary to load balance traffic to one or more firewall farms
- **10-3: SLB Probes:** Explains the configuration steps needed to define probes that test server and firewall farm functionality

10-1: SLB

- SLB provides a virtual server IP address to which clients can connect, representing a group of real physical servers in a server farm. Figure 10-1 shows the basic SLB concept. A client accesses a logical “virtual” server (IP address v.v.v.v), which exists only within the Catalyst 6500 SLB configuration. A group of physical “real” servers (IP addresses x.x.x.x, y.y.y.y, and z.z.z.z) is configured as a server farm. Traffic flows between clients and the virtual server are load balanced across the set of real servers, transparent to the clients.
- As clients open new connections to the virtual server, SLB decides which real server to use based on a load-balancing algorithm.
- Server load balancing is performed by one of these methods:
 - **Weighted round-robin:** Each real server is assigned a weight that gives it the capability to handle connections, relative to the other servers. For a weight n , a server is assigned n new connections before SLB moves on to the next server.
 - **Weighted least connections:** SLB assigns new connections to the real server with the least number of active connections. Each real server is assigned a

weight m , where its capacity for active connections is m divided by the sum of all server weights. SLB assigns new connections to the real server with the number of active connections farthest below its capacity.

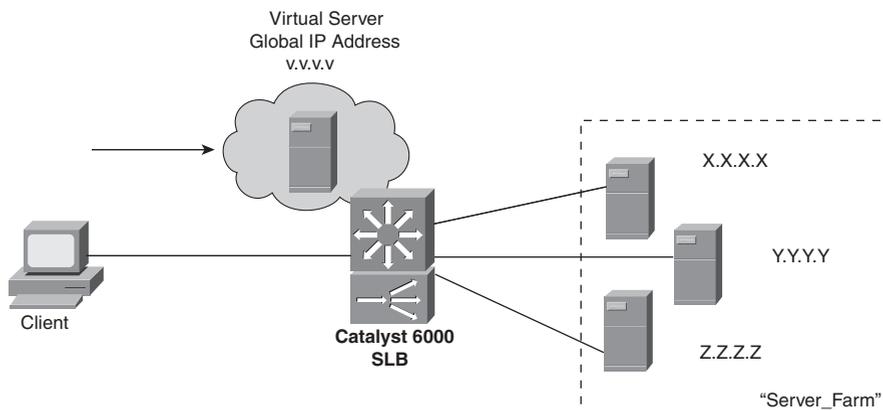


Figure 10-1 SLB Concept

- With weighted least connections, SLB controls the access to a new real server, providing a slow start function. New connections are rate limited and allowed to increase gradually to keep the server from becoming overloaded.
- The virtual server can masquerade as the IP address for all TCP and UDP ports of the real server farm. As well, the virtual server can appear as the IP address of a single port or service of a server farm.
- *Sticky* connections enable SLB to assign new connections from a client to the last real server the client used.
- SLB can detect a real server failure by monitoring failed TCP connections. SLB can take the failed server out of service and return it to service when it is working again.
- SLB can use *server Network Address Translation (NAT)* to translate between the real and virtual server addresses if they reside on different Layer 3 subnets.
- SLB can use *client NAT* to translate the source addresses of client requests into addresses on the server side of the SLB device. This is used when several SLB devices are operating so that return traffic can be sent to the correct SLB device.
- SLB provides a control mechanism over incoming TCP SYN floods to the real servers. This can prevent certain types of denial-of-service attacks.
- SLB can coexist with *Hot Standby Router Protocol (HSRP)* to provide a “stateless backup.” If one SLB router fails, a redundant router can take over the SLB function. However, existing SLB connections will be lost and will have to be reestablished from the client side.

- IOS SLB can also operate as a *Dynamic Feedback Protocol (DFP)* load-balancing manager. The DFP manager collects capacity information from DFP agents running on the real servers.

Configuration

1. Define a server farm.

- a. Assign a name to the server farm:

```
(global) ip slb serverfarm serverfarm-name
```

The server farm is identified by *serverfarm-name* (text string up to 15 characters).

- b. (*Optional*) Select a load-balancing algorithm for the server farm:

```
(server-farm) predictor {roundrobin | leastconns}
```

SLB selects a real server using **roundrobin** (weighted round-robin the default) or **leastconns** (weighted least connections).

- c. (*Optional*) Use server NAT:

```
(server-farm) nat server
```

By default, the virtual server and real server addresses must be Layer 2-adjacent. In other words, SLB forwards packets between the virtual server and a real server by substituting the correct MAC addresses. Server NAT can be used instead, allowing the virtual and real servers to have addresses from separate IP subnets. SLB then substitutes the Layer 3 IP addresses to forward packets between the virtual and real servers, allowing the servers to be separated by multiple routing hops.

- d. (*Optional*) Use client NAT.

- Define a NAT pool of addresses:

```
(global) ip slb natpool pool-name start-ip end-ip {netmask netmask |  
prefix-length leading-1-bits} [entries init-addr [max-addr]]
```

A pool of IP addresses is given the name *pool-name* (text string up to 15 characters), consisting of addresses bounded by *start-ip* and *end-ip*. The subnet mask associated with the pool can be given as a regular subnet mask, *netmask* (x.x.x.x format), or as the number of leading 1 bits in the mask, *leading-1-bits* (1 to 32).

For IOS SLB, client NAT allocates a number of entries as IP addresses and port numbers, *init-addr* (1 to 1,000,000; default 8000) as an initial set to use. When the number of dynamically allocated entries reaches half of the initial number, more entries are allocated. The maximum number of NAT entries can be defined as *max-addr* (1 to 8,000,000; default is the pool size times the number of ports available, or 65,535 to 11,000, or 54,535). Port numbers for translation begin at 11,000.

- Enable client NAT with a pool:

```
(server-farm) nat client pool-name
```

The SLB NAT pool is identified by *pool-name* (up to 15 characters).

- e. (Optional) Assign a unique identifier for DFP:


```
(server-farm) bindid [bind-id]
```

Sometimes, a real server is assigned to multiple server farms. The *bind-id* (0 to 65533; default 0) is an arbitrary identification value given to a server farm. Each instance of a real server references this value, allowing DFP to assign a unique weight to it.
 - f. (Optional) Test the server with a probe:


```
(server-farm) probe name
```

The probe defined as *name* (text string, up to 15 characters) periodically tests for server connectivity and operation. IOS SLB offers ping, HTTP, and *Wireless Session Protocol (WSP)* probes. The CSM also offers TCP, FTP, SMTP, Telnet, and DNS probes. See section “10-3: SLB Probes” for more information about configuring probes.
2. Specify one or more real servers in the server farm.

- a. Identify the real server:

```
(server-farm) real ip-address
```

The real server has the IP address given by *ip-address*.

- b. (Optional) Specify a connection threshold.

- Set the maximum number of connections:

```
(real-server) maxconns number
```

At any given time, the real server will be limited to *number* (1 to 4,294,967,295 connections; default 4,294,967,295) active connections.

- c. (Optional) Assign a relative capacity weight:

```
(real-server) weight weighting-value
```

The real server is assigned a *weighting-value* (1 to 255; default 8) that indicates its capacity relative to other real servers in the server farm. For weighted round-robin, *weighting-value* defines the number of consecutive connections the server receives before SLB moves to the next server. For weighted least connections, the next connection is given to the server whose number of active connections is furthest below its capacity. The capacity is computed as the *weighting-value* divided by the sum of all real server weighting values in the server farm.

- d. *(Optional; IOS SLB only)* Reassign connections when a server doesn't answer:
 (real-server) **reassign** threshold
- SLB attempts to assign a new connection to a real server by forwarding the client's initial SYN. If the server doesn't answer with a SYN handshake before the client retransmits its SYN, an unanswered SYN is recorded. After *threshold* (1 to 4, default 3) unanswered SYNs occur, SLB reassigns the connection to the next server.
- e. *(Optional; IOS SLB only)* Define a failed server threshold:
 (real-server) **faildetect numconns** number-conns [**numclients** number-clients]
- A server is determined to have failed if *number-conns* (1 to 255, default 8 connections) TCP connections have been reassigned to another server. You can also use the **numclients** keyword to specify the *number-clients* (1 to 8, default 2) of unique clients that have had connection failures.
- f. *(Optional; IOS SLB only)* Specify the amount of time before retrying a failed server:
 (real-server) **retry** retry-value
- After a real server has been declared "failed," SLB attempts to assign a new connection to it after *retry-value* (1 to 3600 seconds, default 60 seconds) time has elapsed. You can also use a value of 0 to indicate that new connections should not be attempted.
- g. Allow SLB to begin using the real server:
 (real-server) **inservice**
- By default, the real server is not used by SLB unless it is placed in service. To remove a server from service, use **no inservice**.
3. Define a virtual server for the server farm.
- a. Name the virtual server:
 (global) **ip slb vservice** virtual-server-name
- The virtual server is given the name *virtual-server-name* (text string up to 15 characters).
- b. Assign the virtual server to a server farm:
 (virtual-server) **serverfarm** serverfarm-name
- SLB uses the virtual server as the front end for the server farm named *serverfarm-name* (text string up to 15 characters).
- c. Define the virtual server capabilities:
 (virtual-server) **virtual** ip-address [network-mask] {**tcp** | **udp**} [port | **wsp** | **wsp-wtp** | **wsp-wtls** | **wsp-wtp-wtls**] [**service** service-name]

The virtual server appears as IP address *ip-address* (default 0.0.0.0 or “all networks”) with *network-mask* (default 255.255.255.255).

With IOS SLB, it provides load balancing for the specified **tcp** or **udp** *port*: **dns** or **53** (Domain Name System), **ftp** or **21** (File Transfer Protocol), **https** or **443** (HTTP over Secure Socket Layer), **www** or **80** (HTTP), **telnet** or **23** (Telnet), **smtp** or **25** (SMTP), **pop3** or **110** (POPv3), **pop2** or **109** (POPv2), **nntp** or **119** (Network News Transport Protocol), or **matip-a** or **350** (Mapping of Airline Traffic over IP, type A). A port number of 0 can be given to indicate that the virtual server accepts connections on all ports.

Other alternatives to a port number are **wsp** (connectionless WSP, port 9200), **wsp-wtp** (connection-oriented WSP, port 9201 with WAP FSM), **wsp-wtls** (connectionless secure WSP, port 9202), and **wsp-wtp-wtls** (connection-oriented secure WSP, port 9203).

The **service** keyword can be given to force SLB to assign all connections associated with a given *service-name* (**ftp** or **wsp-wtp**) to the same real server. On a CSM, only **ftp** connections are allowed to be coupled to the originating control session.

- d. *(Optional)* Control access to the virtual server. To allow only specific clients to use the virtual server, enter

```
(virtual-server) client ip-address network-mask
```

Clients having IP addresses within the range given by *ip-address* (default 0.0.0.0, or all addresses) and *network-mask* (default 255.255.255.255, or all networks) are allowed to connect to the virtual server. The *network-mask* in this case resembles the mask of an access list, where a 1 bit ignores and a 0 bit matches. On a CSM, you can use the **exclude** keyword to disallow the IP addresses specified.

- e. *(Optional)* Assign connections from the same client to the same real server:

```
(virtual-server) sticky duration [group group-id] [netmask netmask]
```

For a given client, connections are assigned to the last-used real server for *duration* in seconds (0 to 65,535). Virtual servers can be assigned to a *group-id* (0 to 55; default 0), associating them as a single group. A *netmask* (default 255.255.255.255) can be given such that all client source addresses within the mask are assigned to the same real server.

- f. *(Optional)* Hold connections open after they are terminated:

```
(virtual-server) delay duration
```

After a TCP connection is terminated, SLB can maintain the connection context for *duration* (1 to 600 seconds, default 10 seconds). This can be useful when packets arrive out of sequence, and the connection is reset before the last data packet arrives.

- g. (Optional) Hold connections open after no activity:

```
(virtual-server) idle duration
```

When SLB detects an absence of packets for a connection, it keeps the connection open for *duration* in seconds (IOS: 10 to 65,535; default 3600 seconds or 1 hour) before sending an RST.

- h. (Optional) Prevent a SYN flood to the real servers:

```
(virtual-server) synguard syn-count [interval]
```

SLB monitors the number of SYNs that are received for the virtual server. If more than *syn-count* (0 to 4294967295; default 0 or no SYN monitoring) SYNs are received within the *interval* (50 to 5000 milliseconds; default 100 ms), any subsequent SYNs are dropped.

- i. (Optional) Control the advertisement of the virtual server:

```
(virtual-server) advertise [active]
```

By default, SLB creates a static route for the virtual server address to the Null0 logical interface. This static route can then be redistributed and advertised by a routing protocol. The **active** keyword causes the route to be advertised only when at least one real server is available. You can disable the advertisement with **no advertise**, preventing the static route from being created.

- j. Enable SLB to begin using the virtual server:

```
(virtual-server) inservice [standby group-name]
```

By default, the virtual server is not used by SLB unless it is placed in service. To remove a virtual server from service, use **no inservice**.

Tip You can use multiple IOS SLB devices to provide redundancy for virtual servers. *IOS SLB stateless backup* enables each SLB device to listen to HSRP messages from Layer 3 interfaces on redundant switches. When one switch (and its IOS SLB) fails, another HSRP interface becomes the primary gateway. When the other IOS SLB also detects the failure, the virtual servers that are associated with the HSRP *group-name* (defined previously) become active. No SLB state information is kept, however, so existing connections are dropped and must be reestablished.

Stateless backup requires that HSRP be configured on all the redundant Layer 3 devices on the *server-side* VLAN. Be sure that the *group-name* matches between the HSRP and virtual server configurations. See section “8-6: Router Redundancy with HSRP” in Chapter 8, “Configuring High Availability Features,” for further HSRP configuration information.

- k. (Optional) Use SLB stateful backup:

```
(virtual-server) replicate casa listening-ip remote-ip port-number  
[interval] [password [0/7] password [timeout]]
```

IOS SLB replicates and exchanges its load-sharing decision tables with other stateful backup devices using the *Cisco Appliance Services Architecture*

(CASA) mechanism. When a failure occurs, the backup SLB device already has the current state information and can immediately take over.

This information is sent from the *listening-ip* address (an interface on the local device) to the *remote-ip* address (an interface on the backup device), using TCP port *port-number* (1 to 65,535). Replication messages are sent at *interval* seconds (1 to 300, default 10).

A *password* (text string; use 0 if unencrypted, the default, or 7 if encrypted) can be used for MD5 authentication with the backup device. The optional *timeout* (0 to 65,535 seconds; default 180 seconds) defines a time period when the password can be migrated from an old value to a new one. During this time, both old and new passwords are accepted.

CSM replicates its connection information using the *Content Switching Replication Protocol (CSRP)*. The **sticky** connection database or the regular **connection** database can be replicated. To replicate both, choose each one in a separate **replicate csrp** command.

4. (Optional) Use SLB Dynamic Feedback Protocol (DFP).
 - a. (Optional) Use the DFP manager to communicate with DFP agents on servers.

- Enable the DFP manager:

```
(global) ip slb dfp [password [0|7] password [timeout]]
```

The router can become a DFP load-balancing manager. DFP can be configured with a *password* (text string; use 0 if unencrypted, the default, or 7 if encrypted) for MD5 authentication with a host agent. The optional *timeout* (0 to 65,535 seconds; default 180 seconds) defines a time period when the password can be migrated from an old value to a new one. During this time, both old and new passwords are accepted.

- Specify a DFP agent:

```
(slb-dfp) agent ip-address port-number [timeout [retry-count [retry-interval]]]
```

A DFP agent on a real server is identified by its *ip-address* and the *port-number* number used. The DFP agent (the server) must contact the DFP manager (the IOS SLB device) at *timeout* intervals (0 to 65,535 seconds; default 0 seconds or no timeout period). The DFP manager attempts to reconnect to the agent *retry-count* (0 to 65,535 retries; default 0 retries or an infinite number) times, at intervals of *retry-interval* (1 to 65,535 seconds; default 180 seconds).

- b. (Optional) Use a DFP agent to provide DFP reports.

- Define the agent:

```
(global) ip dfp agent subsystem-name
```

The DFP agent sends periodic reports to its manager, a distributed director device. The *subsystem-name* (text string up to 15 characters) enables the man-

ager to associate the server reports with a subsystem (controlled by the SLB device) for global load balancing. To see what *subsystem-name* values are available from the global manager, use the **ip dfp agent ?** command.

- (Optional) Set a DFP agent password:

```
(dfp) password [0|7] password [timeout]
```

A *password* (text string; use 0 if unencrypted, the default, or 7 if encrypted) can be used for MD5 authentication with a DFP manager. The optional *timeout* (0 to 65,535 seconds; default 180 seconds) defines a time period when the password can be migrated from an old value to a new one. During this time, both old and new passwords are accepted.

- Set the DFP port number:

```
(dfp) port port-number
```

The DFP manager and agents communicate over a common port number, *port-number* (1 to 65535, no default). DFP managers discover their agents dynamically, requiring the port number to be identical between the manager (distributed director) and the agents (IOS SLB).

- (Optional) Set the interval for recalculating weights:

```
(dfp) interval seconds
```

DFP server weights are recalculated at an interval of *seconds* (5 to 65,535 seconds; default 10 seconds) before they are supplied to the DFP manager.

- Enable the DFP agent:

```
(dfp) inservice
```

By default, the DFP agent is disabled.

SLB Example

See Figure 10-2 for a network diagram. SLB is configured to provide load balancing for two server farms: FARM1 and FARM2.

FARM1 is a server farm of three real web servers having IP addresses 192.168.250.10, 192.168.250.11, and 192.168.250.12. The real servers are considered in a “failed” state if four consecutive TCP connections cannot be established with the server. SLB waits 30 seconds before attempting another connection to a failed server. (The number of failed TCP connections and the retry interval are supported only in the IOS command set.) An HTTP probe is configured to try a connection to each real server in the server farm every 120 seconds.

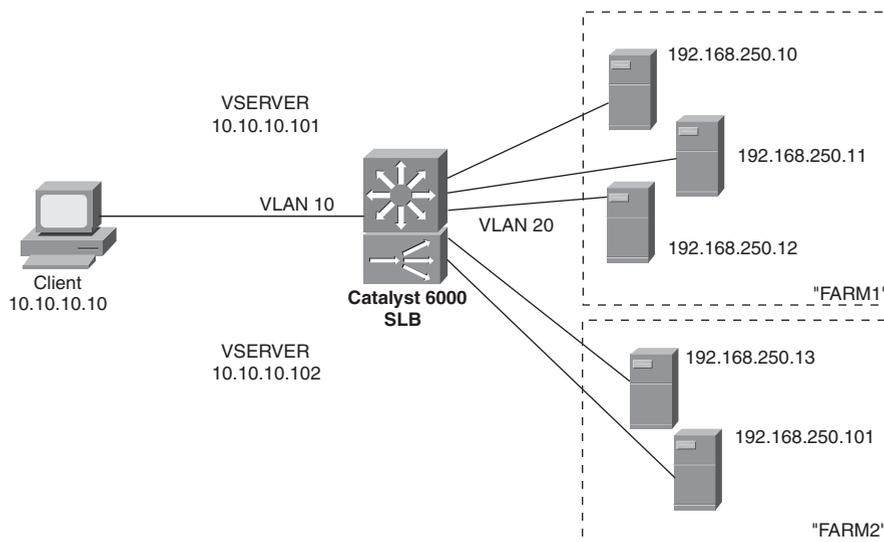


Figure 10-2 Network Diagram for the SLB Example

The virtual server VSERVER1 at 10.10.10.101 uses the weighted least connections algorithm for load balancing between the real servers. New connections are made sticky (passed to the real server last used by the same client) for 60 seconds.

The CSM version of this example also includes the client and server-side VLAN numbers (10 and 20) and IP addresses (10.10.10.2 and 192.168.250.1).

One server is given a weight of 32, one server has a weight of 16, and one server has a weight of 8. New connections are assigned to the server with the least number of active connections, as measured by the server capacities. For example, server 192.168.254.10 has a weight of 32 and a capacity of $32 / (32 + 16 + 8)$ or $32 / 56$. Server 192.168.254.11 has a weight of 16 and a capacity of $16 / (32 + 16 + 8)$ or $16 / 56$. Server 192.168.254.12 has a weight of 8 and a capacity of $8 / (32 + 16 + 8)$ or $8 / 56$. At any given time, the server with the number of active connections furthest below its capacity is given a new connection.

The configuration that follows shows the commands that are necessary for server farm FARM1 and virtual server VSERVER1. The same configuration is shown for an IOS-based switch and a CSM module:

```
(global) ip slb serverfarm FARM1
(server-farm) predictor leastconns
(server-farm) nat server
(server-farm) probe HTTP1
(server-farm) real 192.168.250.10
(real-server) weight 32
```

```
(real-server) faildetect numconns 4
(real-server) retry 30
(real-server) inservice
(real-server) exit
(server-farm) real 192.168.250.11
(real-server) weight 16
(real-server) faildetect numconns 4
(real-server) retry 30
(real-server) inservice
(real-server) exit
(server-farm) real 192.168.250.12
(real-server) weight 8
(real-server) faildetect numconns 4
(real-server) retry 30
(real-server) inservice
(real-server) exit

(global) ip slb vserver VSERVER1
(virtual-server) serverfarm FARM1
(virtual-server) virtual 10.10.10.101 tcp www
(virtual-server) sticky 60 group 1
(virtual-server) advertise active
(virtual-server) inservice
(virtual-server) exit

(global) ip slb dfp password 0 test123
(slb-dfp) agent 192.168.250.10 2000
(slb-dfp) agent 192.168.250.11 2000
(slb-dfp) agent 192.168.250.12 2000
(slb-dfp) exit

(global) probe HTTP1 http
(probe) interval 120
(probe) port 80
(probe) request method get
(probe) exit
```

Displaying Information About SLB

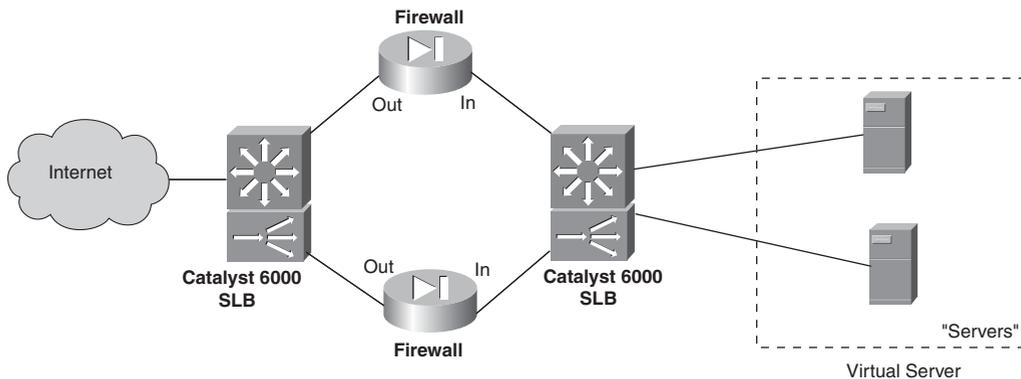
Table 10-1 lists some switch commands that you can use to display helpful information about SLB configuration and status.

Table 10-1 *Commands to Display SLB Configuration and Status Information*

Display Function	Command
Server farms	(exec) show ip slb serverfarms [name <i>serverfarm-name</i>] [detail]
Real servers	(exec) show ip slb reals [vserver <i>virtual-server-name</i>] [detail]
Virtual servers	(exec) show ip slb vsserver [name <i>virtual-server-name</i>] [detail]
SLB connections	(exec) show ip slb conns [vserver <i>virtual-server-name</i> client <i>ip-address</i>] [detail]
DFP status	(exec) show ip slb dfp [agent <i>agent-ip-address</i> port-number manager <i>manager-ip-address</i> detail weights]
SLB redundancy	(exec) show ip slb replicate
Probes	(exec) show ip slb probe [name <i>probe_name</i>] [detail]
SLB statistics	(exec) show ip slb stats

10-2: SLB Firewall Load Balancing

- Firewall load balancing balances traffic flows to one or more firewall farms.
- A firewall farm is a group of firewalls that are connected in parallel or that have their “inside” (protected) and “outside” (unprotected) interfaces connected to common network segments.
- Firewall load balancing requires a load-balancing device (IOS SLB) to be connected to each side of the firewall farm. A firewall farm with “inside” and “outside” interfaces would then require two load-balancing devices, each making sure that traffic flows are directed toward the same firewall for the duration of the connection. Figure 10-3 illustrates the basic firewall load-balancing concept.

**Figure 10-3** *Firewall Load-Balancing Concept*

- Firewall load balancing is performed by computing a hash value of each new traffic flow (source and destination IP addresses and ports). This is called a *route lookup*.
- The firewall load-balancing device then masquerades as the IP address for all firewalls in the firewall farm.
- Firewall load balancing can detect a firewall failure by monitoring probe activity.
- The HSRP can be used to provide a “stateless backup” redundancy for multiple firewall load-balancing devices. If one device fails, a redundant device can take over its function.
- Multiple firewall load-balancing devices can also use “stateful backup” for redundancy. Backup devices keep state information dynamically and can take over immediately if a failure occurs.

Configuration

1. Define a firewall farm.

a. Assign a name to the firewall farm:

```
(global) ip slb firewallfarm firewallfarm-name
```

In IOS SLB, the collection of firewalls is referenced by *firewallfarm-name* (text string up to 15 characters).

b. Identify one or more firewalls in the farm.

■ Specify the firewall’s IP address:

```
(firewall-farm) real ip-address
```

The firewall is directly connected (same logical subnet) to the load-balancing device with an interface at IP address *ip-address*.

■ (Optional) Assign a relative capacity weight:

```
(real-firewall) weight weighting-value
```

The real firewall is assigned a *weighting-value* (1 to 255; default 8) that indicates its capacity relative to other real firewalls in the firewall farm. These values are statically defined and are based on what you think the firewall can handle, relative to the others. The weight values are used only for round-robin or least-connections algorithms.

■ (Optional) Define one or more probes to detect a firewall failure:

```
(real-firewall) probe probe-name
```

The probe that is defined by *probe-name* (text string) is used periodically to determine whether the firewall has failed. Even if more than one probe is defined, the firewall is declared down if it fails just one probe. A firewall must pass all probes to be recovered again.

Tip You must also define the probes separately, as described in section “10-3: SLB Probes.” Ping probes are the most useful for firewall load balancing. For each firewall in the firewall farm, configure a probe to send ping packets that pass completely through the firewall, destined for the firewall load-balancing device on the other side. This tests both “inside” and “outside” interfaces of the firewall, requiring them to be active and operational so that the ping probe is reflected from the other side. Be sure that the firewall is configured to allow ICMP ping packets to pass through.

- Allow load balancing to begin using the firewall:

```
(real-firewall) inserve
```

By default, the real firewall is not used by SLB unless it is placed in service. To remove a firewall from service, use **no inserve**.

- c. (*Optional*) Define one or more flows that will be sent to the firewall farm:

```
(firewall-farm) access [source source-ip-address network-mask]
                 [destination destination-ip-address network-mask]
```

When multiple firewall farms exist, traffic can be identified by address and sent through the appropriate firewall farm. A traffic flow is defined by its source and destination addresses and subnet masks. If either **source** or **destination** keywords are omitted, they default to 0.0.0.0 with a mask of 0.0.0.0, signifying all addresses and networks. This is the default behavior.

- d. (*Optional*) Choose a firewall load-balancing method:

```
(firewall-farm) predictor hash address [port]
```

By default IOS SLB uses the source and destination IP addresses of a flow to select a destination firewall. Use the **port** keyword to use the source and destination addresses, and the source and destination TCP or UDP port numbers, in the selection decision.

- e. (*Optional*) Use stateful backup to recover from a failure:

```
(firewall-farm) replicate casa listening-ip remote-ip port-number
                 [interval] [password [0|7] password [timeout]]
```

The redundant load-balancing devices use CASA structure to exchange and replicate state information. This is sent from the *listening-ip* address (an interface on the local device) to the *remote-ip* address (an interface on the backup device), using *port-number* (1 to 65535). Replication messages are sent at *interval* seconds (1 to 300, default 10).

A *password* (text string; use **0** if unencrypted, the default; or **7** if encrypted) can be used for MD5 authentication with the backup device. The optional *timeout* (0 to 65,535 seconds; default 180 seconds) defines a time period when the password can be migrated from an old value to a new one. During this time, both old and new passwords are accepted.

f. *(Optional)* Adjust the TCP or UDP connection parameters.

- Enter the TCP or UDP configuration mode:

```
(firewall-farm) {tcp|udp}
```

You might need to make adjustments to both TCP and UDP. In this case, this command can be repeated to configure each independently.

- *(Optional; TCP only)* Hold connections open after they are terminated:

```
(firewall-farm-protocol) delay duration
```

After a TCP connection is terminated, the connection context can be maintained for *duration* (1 to 600 seconds, default 10 seconds). This can be useful when packets arrive out of sequence and the connection is reset before the last data packet arrives.

- *(Optional)* Hold connections open after no activity:

```
(firewall-farm-protocol) idle duration
```

When an absence of packets is detected for a connection, the connection is kept open for *duration* (10 to 65,535 seconds; default 3600 seconds or 1 hour) before an RST is sent.

- *(Optional)* Specify the maximum number of connections:

```
(firewall-farm-protocol) maxconns number
```

At any given time, the real server is limited to *number* (1 to 4,294,967,295; default 4,294,967,295) active connections.

- *(Optional)* Assign connections from the same IP address to the same firewall:

```
(firewall-farm-protocol) sticky duration [netmask netmask]
```

For a given IP address, connections are assigned to the last-used firewall for *duration* (0 to 65,535 seconds). A *netmask* can be given so that all source addresses within the mask are assigned to the same firewall.

g. *(IOS SLB only)* Allow firewall load balancing to begin using the firewall:

```
(firewall-farm) inservice
```

By default, the firewall is not used by firewall load balancing unless it is placed in service. To remove a firewall from service, use **no inservice**.

Firewall Load-Balancing Example

To perform firewall load balancing, two load-balancing devices are needed: one located externally and one located internally with respect to the firewall farm. Figure 10-4 shows a network diagram for this example.

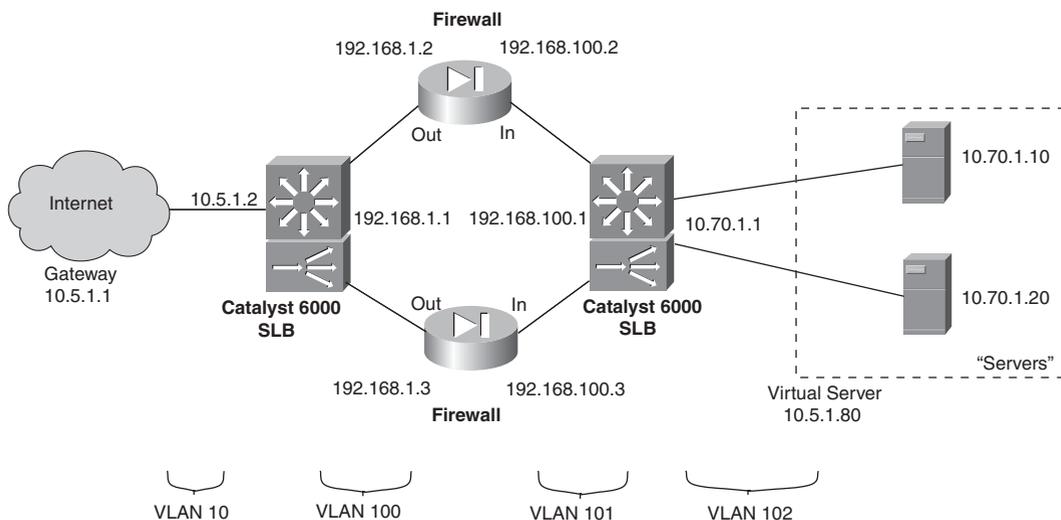


Figure 10-4 Network Diagram for the Firewall Load-Balancing Example

The firewall farm consists of two real firewalls. Their “outside” (unprotected) interfaces are at 192.168.1.2 and 192.168.1.3. Their “inside” (protected) interfaces are at 192.168.100.2 and 192.168.100.3. On the outside, the default gateway is 10.5.1.1, and the external SLB device is at 10.5.1.2.

The internal SLB device performs firewall load balancing for outbound traffic to the firewall farm. As well, it provides normal server load balancing for an internal server farm. The real servers are 10.70.1.10 and 10.70.1.20, and the virtual server appears as 10.5.1.80.

Ping probes are used by both external and internal SLB devices to test for firewall operation. An HTTP probe tests each of the real servers in the server farm. These use the default GET method and are sent every 240 seconds.

The configuration for the external load-balancing device is shown first:

```
(global) ip slb firewallfarm Outside
(firewall-farm) real 192.168.1.2
(real-firewall) weight 8
(real-firewall) probe Ping1
(real-firewall) inservice
(real-firewall) exit
(firewall-farm) real 192.168.1.3
(real-firewall) weight 8
(real-firewall) probe Ping2
(real-firewall) inservice
(real-firewall) exit
(firewall-farm) inservice
(firewall-farm) exit
```

```
(global) ip slb probe Ping1 ping
(probe) address 192.168.100.1
(probe) interval 10
(probe) faildetect 4
(global) ip slb probe Ping2 ping
(probe) address 192.168.100.1
(probe) interval 10
(probe) faildetect 4
(probe) exit
```

Now the configuration for the internal load-balancing device is shown:

```
(global) ip slb firewallfarm Inside
(firewall-farm) real 192.168.100.2
(real-firewall) weight 8
(real-firewall) probe Ping1
(real-firewall) inservice
(real-firewall) exit
(firewall-farm) real 192.168.100.3
(real-firewall) weight 8
(real-firewall) probe Ping2
(real-firewall) inservice
(real-firewall) exit
(firewall-farm) inservice
(firewall-farm) exit

(global) ip slb serverfarm Servers
(server-farm) nat server
(server-farm) probe HTTP1
(server-farm) real 10.70.1.10
(real-server) inservice
(real-server) exit
(server-farm) real 10.70.1.20
(real-server) inservice
(real-server) exit

(global) ip slb vserver Vservers
(virtual-server) serverfarm Servers
(virtual-server) virtual 10.5.1.80 tcp 0
(virtual-server) inservice
(virtual-server) exit

(global) ip slb probe Ping1 ping
(probe) address 192.168.1.1
(probe) interval 10
```

```

(probe) faildetect 4
(probe) exit
(global) ip slb probe Ping2 ping
(probe) address 192.168.1.1
(probe) interval 10
(probe) faildetect 4
(probe) exit
(global) ip slb probe HTTP1 http
(probe) port 80
(probe) interval 240
(probe) request

```

Displaying Information About Firewall Load Balancing

Table 10-2 lists some switch commands that you can use to display helpful information about SLB firewall load-balancing configuration and status.

Table 10-2 *Commands to Display SLB Firewall Load-Balancing Configuration and Status Information*

Display Function	Command
Status of firewalls in a farm	(exec) show ip slb reals
Firewall weight and connection counters	(exec) show ip slb reals detail
Firewall farm status	(exec) show ip slb firewallfarm
Load-balancing connections to firewalls	(exec) show ip slb conns [firewall firewallfarm-name] [detail]
Probes	(exec) show ip slb probe [name probe_name] [detail]
Sticky connections	(exec) show ip slb sticky

10-3: SLB Probes

- Probes can be used to test for server or firewall connectivity and proper operation.
- Probes can be defined to simulate requests for these protocols:
 - ICMP: Sends ICMP echo (ping) requests to a real server.
 - HTTP: Sends HTTP requests to a real server, using TCP port 80.
 - WSP: Requests and verifies the replies using Wireless Access Protocol (WAP), port 9201.
 - Telnet: Opens and closes a Telnet connection (TCP port 23) to a real server.
 - TCP: Establishes and resets TCP connections to a real server. This can be used to support any TCP port, including HTTPS or SSL, port 443.

- FTP: Opens and closes an FTP connection (TCP ports 20 and 21) to a real server.
- SMTP: Opens and closes an SMTP connection (TCP port 25) to a real server.
- DNS: Sends requests to and verifies the replies from a real DNS server.

Configuration

1. Define the probe:

```
(global) ip slb probe name {ping | http | wsp}
```

The probe is named *name* (text string up to 15 characters) and can be referenced by other SLB server and firewall farm commands. IOS SLB allows these probe types: **ping** (ICMP), **http**, or **wsp** (WAP port 9201). (*Optional*) Define the target address:

```
(probe) address [ip-address]
```

For a server farm, this command is not used. The *ip-address* used by the probe is inherited from each real server in the server farm. With IOS SLB, addresses are not inherited when the probe is used for a firewall farm. You must use this command to define the address of a target firewall.

2. Set the probe behavior:
 - a. (*Optional*) Set the time between probes:

```
(probe) interval seconds
```

Probes are sent toward the target at intervals of *seconds* (IOS SLB: 1 to 65,535 seconds; default 1 second; CSM: 5 to 65,535 seconds; default 120 seconds).

- b. (*Optional*) Define the criteria for a failure:

```
(probe) faildetect retry-count
```

With IOS SLB, a server or firewall is considered to have failed if *retry-count* (1 to 255; default 10) consecutive ping probes are unanswered. With a CSM, the target has failed if *retry-count* (0 to 65,535; default 3) probes of any type are unanswered.

3. (*Optional; HTTP probe only*) Define the HTTP probe operation:

- a. (*Optional*) Set the port number:

```
(probe) port port-number
```

Usually, an HTTP probe uses *port-number* 80. If the *port-number* is unspecified, however, it is inherited from the virtual server. For a firewall probe, the *port-number* must be given (1 to 65,535). The target device must answer an HTTP request for the probe to work.

- b. (*Optional*) Define the HTTP probe method:

```
(probe) request [method {get | post | head | name name}] [url path]
```

The probe requests information from the server using the **get** (the default), **post**, **head** (request a header data type), or **name** (request the data named *name*) method. A URL can also be given, specifying the server *path* (text string URL; default */*).

- c. (Optional) Specify the probe header information:

```
(probe) header field-name [field-value]
```

The probe header name is set to *field-name* (text string up to 15 characters), with a value of *field-value*. A colon is automatically inserted between the name and value. By default, the request contains these headers:

```
Accept: */*
```

```
Connection: close
```

```
User-Agent: cisco-slb-probe/1.0
```

```
Host: virtual-IP-address
```

- d. (Optional) Specify the HTTP authentication values:

```
(probe) credentials username [password]
```

If HTTP authentication is required, a *username* (text string, up to 15 characters) and a *password* (text string up to 15 characters) can be given for the probe.

- e. (Optional) Expect a specific status code to be returned:

```
(probe) expect [status status-code] [regex regular-expression]
```

A real server or a firewall is considered to have failed if it either does not respond to an HTTP probe or if it returns a *status-code* (100 to 599, default 200) other than the one specified. For firewalls, the *status-code* should be set to 401. For a CSM, the status code must be within the range *min-number* (default 0) and *max-number* (optional, default 999).

With IOS SLB, you can also expect a regular expression along with the status code. Use the **regex** keyword and specify a *regular-expression* (text string, no default). Only the first 2920 bytes of the probe reply are searched for a match.

4. (Optional; WSP probe only) Define the target URL:

```
(probe) url [path]
```

A URL can also be given, specifying the server *path* (text string URL; default */*).

Displaying Information About SLB Probes

To display helpful configuration and status information about SLB probes, enter the following command:

```
(exec) show ip slb probe [name probe_name] [detail]
```

Index

Symbols

- (*, G) common shared tree structure, 141
- (S, G) shortest path tree structure, 141
- 6000 series Catalyst switches, password recovery process, 33-34
- 802.1Q trunking, native VLAN switching, 96
- 802.1X port authentication, configuring, 186

A

- access layer, 17-18
 - configuring for voice QoS, 256-259
- access ports, 91
- accessing
 - modules, 34
 - switch devices, SSH, 184-185
- ACEs (access control entries), 227
- ACLs (access control lists)
 - configuring, 183-184
 - VACLs, 176-178
- active commands, disabling, 3
- adding entries to switching table, 53-54
- AF (Assured Forwarding) service levels, 223
- aggressive mode (UDLD), 115
- aging time, configuring on switching table, 54
- assigning IP management address, 28
- assigning VLAN ports
 - dynamic assignment, 91-93
 - static, 91
- asynchronous back-to-back connections, 268
- authentication
 - configuring, 180
 - example, 182
 - port authentication, configuring, 185-186
 - RADIUS, configuring, 181-182
 - TACACS, configuring, 181
- automatic IP management address assignment, 28

B

back-to-back connections

asynchronous, 268

Ethernet, 267

T1/E1 CSU/DSU, 269

backward compatibility, alias commands, 41

banners, configuring, 26

BID (bridge ID), 112

blocking state (STP), 114

boot parameters, synchronizing on Supervisor Engine, 45

booting

from ROM Monitor, 11

images from Flash, 40-41

BPDU filtering, 126

BPDU skewing, 124-126

BPDU (Bridge Protocol Data Units), TC bit set, 114

broadcast domains, design principles, 21

broadcast suppression, 168

configuring, 168-169

verifying configuration, 170

building blocks of network design, 18-20

BVI (bridged virtual interface), 82

C

card modules, Supervisor redundancy, 42

Catalyst 2000 series switches, 13

Catalyst 2900XL/3500XL, configuring QoS, 228

Catalyst 3000 series switches, 14-15

Catalyst 3500XL switches, creating private edge VLANs, 106-107

Catalyst 4500 series switches, 15-16

Catalyst 6500 series routers, 16

Enhanced FlexWAN interfaces, configuring, 78-79

POS interfaces, configuring, 80

SIP interfaces, configuring, 79-80

cd command, 37

CDP (Cisco Discovery Protocol), 23

configuring, 46-47

version 2, 96

changing VTP versions, 102

channel-group command, 75

character limitations of banners, 26

CIR (committed information rate), 234

Cisco Blade Switch 3100 series, 14

Cisco Field Manual: Router

Configuration (Cisco Press), 48, 73

Cisco IOS Software

command line, editing, 3

command output, searching, 4-5

context-sensitive help, 3-4

regular expressions, 5

terminal sessions, 6-7

user interface features, 3

user modes, 2

web browser interface, configuring, 8-9

Cisco IP Phone, initialization process, 250

class maps, QoS, 239-244

classification

Layer 2 frames, 222-223

Layer 3 frames, 223-226

clearing modules, 35

- clock update-calendar command, 49
- collapsed core design, 17
- collecting RMON statistics, 204-205
- command set (ROM Monitor), 9-11
- commands
 - cd, 37
 - channel group, 75
 - clock update-calendar, 49
 - copy, 39-40
 - enable secret, 30
 - format, 39
 - ip address, 85
 - ip domain-lookup, 28
 - more, 4
 - ping, verifying packet reachability, 215-216
 - recalling, 4
 - redundancy force-switchover, 44
 - regular expressions, 5
 - reload, 44
 - router, 85
 - service config, 28
 - service password-encryption, 30
 - session, 34
 - set spantree channelvlancost, 64
 - show cdp, 46
 - show channel group, 63
 - show etherchannel, 77
 - show interfaces, 61, 77
 - show interfaces trunk, 97
 - show ip route default, 28
 - show module all, 45
 - show redundancy states, 132
 - show running-config, 3
 - show sessions, 6
 - show spantree, 251
 - switchport, 72
 - switchport host, 252
 - switchport mode trunk, 99
 - switchport trunk encapsulation, 96
 - traceroute, 216-218
 - undelete, 38
 - vlan allocation policy, 89
- community string values, configuring
 - SNMP access, 200-201
- community VLANs, creating, 105
- configuration files (SNMP), saving to
 - TFTP server, 203
- configuration mode, 2
- configuring
 - ACLs, 183-184
 - broadcast suppression, 168-169
 - CDP, 46-47
 - Cisco IOS Software, Web browser interface, 8-9
 - DARP, 191
 - default gateway, 28
 - DNS services, 28-29
 - firewall load balancing, 159-163
 - HSRP, 136-137
 - HTTP services, 29
 - IGMP snooping, 143-144
 - IP management address, 27-28
 - Layer 2 interfaces
 - Layer 2 interfaces
 - EtherChannel*, 62-67
 - Ethernet*, 57-60
 - port selection*, 56-57
 - switching table information, displaying*, 53-55
 - Layer 3 EtherChannels, 74-75
 - example configuration*, 77-78
 - verifying configuration*, 76-77
 - Layer 3 Ethernet interfaces, 72-73

- NSF, 133-134
- packet tracing, 215-216
- passwords, 30
- port authentication, 185-186
- port security, 173-175
- power supply redundancy, 213
- protocol filtering, 171
- QoS
 - access layer, configuring, 256-259*
 - class maps, 239-244*
 - congestion avoidance, 244-245*
 - core layer, configuring, 259*
 - data exports, 246-248*
 - distribution layer, configuring, 259-261*
 - ingress port queues, 231-233*
 - microflow policers, 234-235*
 - on Catalyst 2900XL/3500XL, 228*
 - policies, 237-238*
 - port-based traffic classification, 229-231*
- routing tables, 85-86
- RPR, 131-132
- RSPAN, 208-210
- SLB, 149-155
 - probes, 164-166*
- SNMP, 199-203
 - example, 205-206*
 - notifications, 203*
 - RMON support, 204-205*
 - traps, 203-204*
- SPAN, 206-210
- SSH, 184-185
- SSO, 133-134
- STP, 116-120
 - timers, 124-126*
- Supervisor Engine
 - banners, 26*
 - prompts, 25*
- switch authentication, 180
 - RADIUS, 181-182*
 - TACACS, 181*
- syslog, 194-198
- system time, 48-50
- terminal sessions, timeout values, 7
- trunking, 93-94
- trunks
 - encapsulation method, 95-96*
 - removing VLANs from trunk links, 96-97*
- VACLs, 176-178
- virtual interfaces
 - example configuration, 84-85*
 - subinterfaces, 83-84*
 - verifying configuration, 84*
 - VLAN interfaces, 82*
- VLANs
 - dynamic port assignment, 91-93*
 - private edge VLANs, 106-107*
 - private VLANs, 105-106*
 - static port assignment, 91*
- voice ports, IP phone support, 250-253
- VTP, 88, 98-99
 - changing versions, 102*
 - example, 103-104*
 - modes, 100-101*
 - pruning, 101-102*
 - setting passwords, 99-100*
 - verifying operation, 102*
- WAN interfaces, 78
 - Enhanced FlexWAN interface, 78-79*

- example configuration, 81-82*
- POS, 80*
- SIP module, 79-80*
- verifying configuration, 81*
- congestion avoidance, configuring, 244-245
- connections, back-to-back
 - asynchronous, 268
 - Ethernet, 267
 - T1/E1 CSU/DSU, 269
- connector pinouts, 266
- context-sensitive help, Cisco IOS Software, 3-4
- controlling traffic. protocol filtering
 - example, 172-173
 - verifying configuration, 171
- copy command, 39-40
- copying system files, 39-40
- core layer, 17
 - configuring for voice QoS, 259
 - redundancy, 20
- creating
 - community VLANs, 105
 - isolated VLANs, 105
 - private edge VLANs, 106-107
 - VLANs, 88
 - example, 90-91*
 - extended range, 89-90*
 - standard range, 89*
- crossover cables, 267
- CST (Common Spanning Tree), 111

D

- DAI, 22
- DARP, 191
- databases (VTP), configuring, 88

- date and time, system calendar configuration, 49
- debouncing port state changes, 59
- default gateway, configuring, 28
- default port costs, 113-114
- default VLAN, 91
- deleting files from Flash, 38-39
- design principles of switched networks, 17-22
- designated port election (STP), 112
- deterministic frame distribution, 62
- DFP (Dynamic Feedback Protocol) manager, enabling, 154-155
- DHCP (Dynamic Host Configuration Protocol), 173, 224
- DHCP snooping
 - example, 189
 - verifying configuration, 190
- DHCP starvation attacks, 187
- DiffServ, 223
- disabled state (STP), 114
- disabling
 - active commands, 3
 - DTP on trunks, 94
 - HTTP server, 8
 - modules, 35
- displaying
 - file system devices, 36-38
 - firewall load balancing information, 164
 - HSRP information, 138
 - installed modules, 34
 - Layer 2 interface information, 61-62
 - logging information, 198
 - NSF information, 135
 - power management information, 214
 - QoS information, 245

- RPR information, 132
- SLB information, 157
- SLB probe information, 166
- SNMP information, 206
- SPAN information, 211-213
- SSO information, 135
- STP information, 120
- switching table information, 54-55
- terminal sessions, 6
- voice port information, 253
- distribution layer, 17-18**
 - configuring for voice QoS, 259-261
- DNS services, configuring, 28-29**
- domain names, VTP, 99**
- domains, QoS, 221**
- drop precedence categories (AF), 223**
- DSCP (Differentiated Services Code Point), 223**
 - class selector, 223
 - fields, 224-225
 - internal values, mapping to egress CoS values, 244
- DTP (Dynamic Trunking Protocol)**
 - disabling on trunks, 94
 - trunking mode characteristics, 95
- dynamic port assignment (VLANs), 91-93**
- dynamic pruning (VTP), 101**

E

- editing IOS command line, 3
- EF (Expedited Forwarding) class, 224**
- EHSA (Enhanced High System Availability), 45**
- election processes (STP), 112**
- enable secret command, 30**
- enabling trunking, 94**
- encapsulation method, specifying on trunks, 95-96**
- ending terminal sessions, 7**
- Enhanced FlexWAN module, configuring, 78-79**
- environment monitoring, 214**
- EtherChannel, 62**
 - configuring, 63-67
 - example configuration, 67
 - Layer 3
 - configuring, 74-75*
 - example configuration, 77-78*
 - verifying configuration, 76-77*
- Ethernet**
 - back-to-back connections, 267
 - configuring, 57-60
 - example configuration, 60
 - Jumbo frame support, 59
 - Layer 3 interfaces
 - configuring, 72-73*
 - example configuration, 73*
 - verifying configuration, 73*
 - type codes, 310-316
 - VLANs, configurable parameters, 88
- examples**
 - of banners, 26
 - of CDP configuration, 47
 - of HTTP services, 29
 - of IGMP snooping, 145
 - of protocol filtering, 172-173
 - of DHCP snooping, 189
 - of EtherChannel configuration, 67
 - of Ethernet configuration, 60
 - of firewall load balancing, 162-164
 - of Layer 3 EtherChannel configuration, 77-78

- of Layer 3 interface configuration, 73
- of packet tracing, 218
- of port security, 175, 188
- of port selection, 57
- of private VLANs, 107-109
- of SLB, 155-157
- of SNMP configuration, 205-206
- of SPAN configuration, 210
- of STP operation, 115-116
 - load balancing*, 122-123
 - poor root placement*, 120-122
- of switch authentication, 182
- of system time configuration, 50
- of switching table configuration, 54-55
- of trunks, 97-98
- of VACLs, 178-180
- of virtual interface configuration, 84-85
- of VLAN configuration, 90-91
- of VTP configuration, 103-104
- of WAN interface configuration, 81-82
- exporting QoS data, 246-248
- extended range, VLAN numbers, 88
- extended VLANs, 88-90

F

- facility types (syslog servers), 195
- features of Cisco IOS user interface, 3
- FEC (Fast EtherChannel), 62
- file systems
 - alias command, 41
 - deleting files from Flash, 38-39

- Flash memory, booting images from, 40-41
 - system files, moving, 39-40

filtering

- Cisco IOS command output, 4-5
- traffic, VACLs, 176-178

firewall load balancing

- configuring, 159-163
- displaying information, 164
- example, 162-164

Flash memory

- booting images from, 40-41
- removing files, 38-39

FlexWAN modules, enabling extended VLANs, 90

format command, 39

Forward Delay interval, adjusting, 125

Forward Delay timer (STP), 124

forwarding state (STP), 114

frames

- deterministic distribution, 62
- Layer 2 classification, 222-223
- Layer 3 marking, 223-224, 226

FSU (Fast Software Upgrade), performing, 138-139

G-H

GARP (Gratuitous ARP), 187

GEC (Gigabit EtherChannel), 62

group membership, IGMP join requests, 143

hardware clock, configuring, 49

Hello timer, adjusting, 125

Hello timer (STP), 124

help (IOS), context-sensitive, 3-4

hierarchy of switched networks, 17-18

building blocks of network design, 19

high availability

NSF, 132

configuring, 133-134

displaying information about, 135

RPR

configuring, 131-132

displaying information, 132

SSO, 132

configuring, 133-134

displaying information about, 135

HSRP (Hot Standby Router Protocol), 135

configuring, 136-137

displaying information, 138

example, 137-138

HTTP server, disabling, 8

HTTP services, 29



ICMP type codes, 281-284

IEEE 802.1 trunks, 222

IFS (IOS file system), 35

alias commands, backward compatibility, 41

deleting file from Flash, 38-39

Flash memory, booting images from, 40-41

navigating, 36-38

system files, moving, 39-40

IGMP Fast-Leave Processing, 143

IGMP snooping, 142-143

configuring, 143-144

displaying information, 145

example, 145

images

booting from flash memory, 40-41

IOS Supervisor Engine, synchronizing, 44

improving STP stability, 115

in-profile traffic, 227

inbound vty, configuring ACLs, 183-184

ingress port queues (QoS), configuring, 231-233

initialization process, Cisco IP Phone, 250

inline power, voice ports, 249

installed modules, viewing, 34

internal DSCP value

applying to QoS theory, 222

mapping to egress CoS values, 244

IOS devices, forcing changes in standby Supervisor, 44

IOS SLB stateless backup, 153

IOS VACLs, configuring, 176-178

IOS-based switches, configuring STP, 116-120

ip address command, 85

ip domain-lookup command, 28

IP management address

configuring, 27-28

DNS services, configuring, 28-29

HTTP services, configuring, 29

IP phone support, configuring on voice ports, 250-253

IP precedence, fields, 224-225

ISL trunks, 223

isolated VLANs, creating, 105

J-K-L

join requests, 142-143

jumbo frame support on Ethernet interfaces, 59

LACP, 62, 67

load balancing, firewall load balancing, 159

Layer 2 classification, 222-223

Layer 2 interfaces

displaying information, 61-62

EtherChannel

configuring, 62-66

example configuration, 67

Ethernet

configuring, 57-59

example configuration, 60

jumbo frame support, 59

port selection, configuring, 56-57

switching table

configuring, 53-54

example configuration, 54-55

information, displaying, 54-55

Layer 3 classification, 223-224, 226

Layer 3 EtherChannels

configuring, 74-75

example configuration, 77-78

verifying configuration, 76-77

Layer 3 Ethernet interfaces

configuring, 72-73

example configuration, 73

verifying configuration, 73

learning state (STP), 114

listening state (STP), 114

LLDP, 23

LLDP-Med, 23

load balancing

example of, 122-123

firewall load balancing

configuring, 159-163

displaying information, 164

example, 162-164

SLB, 147-148

configuring, 149-155

displaying information, 157

example, 155-157

SLB probes, configuring, 164-166

logging, 193

syslog

configuring, 194-198

displaying information, 198

long mode default port costs, 113-114

loop detection, STP example, 115-116

loop prevention, STP, 111

BID, 112

configuring, 116-120

convergence tuning, 124-126

displaying information, 120

election processes, 112

load balancing, example of, 122-123

path costs, 113-114

poor root placement, example of, 120-122

port states, 114

stability, improving, 115

TC bit set, 114

tiebreakers, 113

topology changes, 114

topology navigation, 127-130

M

manual system time configuration, 48-49
mapping internal DSCP values to egress CoS values, 244
marking
 Layer 2 frames, 222-223
 Layer 3 frames, 223-226
MaxAge timer, adjusting, 125
MaxAge timer (STP), 124
maximum cabling distances, 263-265
messages, logging, 193
 syslog, configuring, 194-198
 syslog, displaying information, 198
microflow policers, configuring, 234-235
microflows, 227
modes of VTP operation, 100-101
modules
 accessing, 34
 powering on/off, 35
 resetting, 35
 viewing, 34
monitoring environmental conditions, 214
more command, 4
moving system files, 39-40
MST (Multiple Spanning Tree), 112
MTU (maximum transmission unit), 59
mtu parameter, configuring Ethernet VLANs, 89
multicast addressing
 IGMP snooping, 142-145
 tree structures, 141
multicast broadcast floods, controlling, 169

N

name parameter, configuring Ethernet VLANs, 89
native VLAN (802.1Q), switching, 96
navigating
 IFS, 36-38
 STP topology, 127-130
nested Telnet sessions, 6
network management, SNMP, 199
 configuring, 199-202
 displaying information, 206
 example, 205-206
 notifications, 203
 RMON support, 204-205
 saving configuration file to TFTP server, 203
 traps, 203-204
network media
 connector pinouts, 266
 maximum cabling distances, 263-265
normal mode (UDLD), 115
normal range, VLAN numbers, 88
notifications, SNMP, 203-204
NSF (Non-Stop Forwarding), 132
 configuring, 133-134
 displaying information about, 135
NSF/SSO mode, 43
NTP (Network Time Protocol)
 stratum, 47
 system time, configuring, 49-50

O-P

operating systems, alias command backward compatibility, 41
out-of-profile traffic, 227

packets, tracing, 215-218

passwords

- privileged, configuring, 30
- recovering on 6000 series Catalyst switches, 33-34
- recovering on switches, 31-32
- setting for VTP, 99-100
- user-level, configuring, 30

path costs (STP), 113-114

pause frames, 58

PHB, 224

ping command, verifying packet reachability, 215-216

pinouts, 266

policies (QoS), configuring, 237-238

policing traffic, 227

- microflow policers, configuring, 234-235

poor root placement (STP), example of, 120-122

port assignment, verifying on VLANs, 93

port authentication, configuring, 185-186

port channels, 74

port security, 188

- configuring, 173-174
- example, 188
- example of, 175
- verifying configuration, 175, 188
- violations, 174

port states, STP, 114

ports

- Layer 2, selecting, 56-57
- trunking, 94-96
- VLAN
 - dynamic assignment*, 91-93
 - static assignment*, 91

POS interfaces, configuring, 80

power supply redundancy

- configuring, 213
- displaying information, 214

powered devices, inline power, 249

powering modules on/off, 35

primary Supervisor, changing backup Supervisor configuration, 44

private edge VLANs, creating, 106-107

private VLANs

- configuring, 105-106
- example configuration, 107-109
- verifying operation, 107

privileged EXEC mode, 2

privileged passwords, configuring, 30

prompts, configuring on Supervisor Engine, 25

protected ports, creating private edge VLANs,

106-107

protocol filtering

- configuring, 171
- example, 172-173
- verifying configuration, 171

pruning, VTP, 101-102

PVST+, 112

Q

QoS

- configuring on Catalyst 2900XL/3500XL, 228
- congestion avoidance, configuring, 244-245
- DHCP, PHBs, 224
- DiffServ, 223
- displaying information, 245

- domains, 221
- DSCP fields, 224-225
- exporting data, 246-248
- for voice traffic, 254-255
 - access layer, configuring, 256-259*
 - core layer, configuring, 259*
 - distribution layer, configuring, 259-261*
 - voice control protocols, 255-256*
- ingress port queues, configuring, 231-233
- internal DSCP values, 222
 - mapping to egress CoS values, 244*
- Layer 2 classification and marking, 222-223
- Layer 3 classification and marking, 223-226
- microflow policers, configuring, 234-235
- network design principles, 22
- policies, 237-238
 - class maps, 239-244*
- policing, 227
- port-based traffic classification, 229-231
- queuing, 226

queuing, 226

R

- RADIUS, configuring switch authentication, 181-182
- Rapid PVST+, 112
- reachability, verifying with ping command, 215-216
- recalling commands, 4
- recipients of SNMP notifications, defining, 203
- recovering lost passwords, 31-32
 - on 6000 series Catalyst switches, 33-34
- redundancy
 - HSRP
 - configuring, 136-137*
 - example, 137-138*
 - of network building blocks, 20
 - Supervisor Engine slots, 42
 - in switch modules, 22
- redundancy force-switchover command, 44
- redundant power supplies
 - configuring, 213
 - displaying information, 214
- regular expressions, Cisco IOS command line, 5
- reload command, 44
- removing
 - files from Flash, 38-39
 - VLANs from trunk links, 96-97
- resetting modules, 35
- restricting vty access, 183-184
- resuming terminal sessions, 6
- RMON, 199
 - history statistics, collecting, 204-205
- rollover cables, 268
- ROM Monitor, 9
 - booting from, 11
 - command set, 9-11
 - configuration variables, saving, 10
- route lookup, 159
- router command, 85
- router discovery, traceroute command, 216-218

routing tables

- configuring, 85-86

- verifying configuration, 86

RPR (Route Processor Redundancy)

- configuring, 131-132

- information, displaying, 132

RPR mode, 42**RPR+ mode, 42****RSPAN, configuring, 208-210****RTP (Real-Time Transport Protocol), 255****S**

saving ROM Monitor configuration variables, 10**scaling trunks, 21****SCCP (Skinny Client Control Protocol), 255-256****searching IOS command output, 4-5****security**

- DARP, 191

- port authentication, configuring, 185-186

- port security, 188

- configuring, 173-174*

- example of, 175, 188*

- verifying configuration, 175, 188*

- violations, 174*

- SNMP, defining policies, 202

- SSH, configuring, 184-185

- switch authentication, 180

- example, 182*

- RADIUS, 181-182*

- TACACS, 181*

- VACLs, 176

- configuring, 176-178*

- verifying configuration, 178*

- selecting Layer 2 ports, 56-57

- server blocks, 20

- server farms, SLB, 147-148

- configuring, 149-155

- displaying information, 157

- example, 155-157

- probes, configuring, 164-166

- server mode (VTP), 99

- service config command, 28

- service password-encryption command, 30

- session command, 34

- set spantree channelvlancost command, 64

- severity levels of syslog messages, 196

- short mode default port costs, 113-114

- show cdp command, 46

- show channel group command, 63

- show etherchannel command, 77

- show interfaces command, 61, 77

- show interfaces trunk command, 97

- show ip route default command, 28

- show module all command, 45

- show redundancy states command, 132

- show running-config command, 3

- show sessions command, 6

- show spantree command, 251

- SIP (SPA Interface Processor) modules, 78

- configuring, 79-80

- SLB (Server Load Balancing), 147-148, 159

- configuring, 149-155

- displaying information, 157

- example, 155-157

- probes

- configuring, 164-166*
- information, displaying, 166*
- SNMP (Simple Network Management Protocol)**
 - access, configuring, 200-201
 - configuration files, saving, 203
 - configuring, 199-200, 202
 - displaying information, 206
 - example configuration, 205-206
 - notifications, traps, 203-204
 - RMON support, 204-205
- SPAN**
 - configuring, 206-208
 - displaying information, 211-213
 - example, 210
 - RSPAN, configuring, 208-210
- Spanning-Tree MAC reduction, enabling on extended VLANs, 90**
- SRM/SSO mode, 43**
- SSH (Secure Shell), configuring, 184-185**
- SSO (Supervisor Switchover), 132**
 - configuring, 133-134
 - displaying information about, 135
- stability of STP, improving, 115**
- standard VLANs, 88-89**
- standby Supervisor, system redundancy, 42**
- state parameter, configuring Ethernet VLANs, 89**
- stateless backup, 153**
- static port assignment (VLANs), 91**
- STP (Spanning Tree Protocol), 111**
 - BID, 112
 - BPDU, TC bit set, 114
 - configuring, 116-120
 - convergence tuning, 124-126
 - displaying information, 120
 - election processes, 112
 - example, 115-116
 - load balancing, example, 122-123
 - path costs, 113-114
 - poor root placement, example, 120-122
 - port states, 114
 - stability, improving, 115
 - tiebreakers, 113
 - topology changes, 114
 - topology navigation, 127-130
- STP BackboneFast, 124**
- STP Root Guard, enabling, 118**
- STP UplinkFast, 124**
- stratum, 47**
- subinterfaces, configuring, 83-84**
- Supervisor Engine**
 - banners, configuring, 26
 - forcing changes in backup Supervisor, 44
 - FSU, performing, 138-139
 - IOS images, synchronizing, 44
 - modes of operation, 42-43
 - prompts, configuring, 25
 - SSO, 132
 - synchronizing boot parameters, 45
 - system redundancy, 42
- switch authentication**
 - configuring, 180
 - example, 182
 - RADIUS, configuring, 181-182
 - TACACS, configuring, 181
- switch blocks, 20-21**
- switch modules, redundancy, 22**
- switch port trunk encapsulation command, 96**

switch ports, discarding STP port states, 114

switched networks, design principles, 17-22

switches

- booting in rommon mode, 11
- EtherChannel
 - configuring*, 63-67
 - example configuration*, 67
- password recovery process, 31-32

switching VTP versions, 102

switching table

- aging time, configuring, 54
- configuring, 53
- example configuration, 54-55
- information, displaying, 54-55

switchport command, 72

switchport host command, 252

switchport mode trunk command, 99

synchronizing IOS images, 44

synchronizing boot parameters on Supervisor Engine, 45

synchronous logging, 197

syslog

- configuring, 194-198
- displaying information, 198

system time

- configuring with NTP, 49-50
- manual configuration, 48-49

T

T1/E1 CSU/DSU back-to-back connections, 269

TACACS, configuring switch authentication, 181

TC bit set, 114

TCN BPDUs, 114

Telnet

- SSH, configuring, 184-185
- vty access, restricting, 183-184

temperature monitoring, 214

terminal sessions, 6

- displaying, 6
- ending, 7
- resuming, 6
- timeout values, configuring, 7

tiebreakers (STP), 113

timers, STP convergence tuning, 124-126

token bucket algorithm, 227

TopN reports, 61-62

topology changes (STP), 114

ToS byte, 223

traceroute command, 216-218

tracing packets, 215-218

traffic

- broadcast suppression, 168
 - configuring*, 168-169
 - verifying configuration*, 170
- controlling with protocol filtering, 171
- in-profile, 227
- out-of-profile, 227
- policing, 227

transferring system files, 39-40

traps (SNMP), configuring, 203-204

trunks, 98

- configuring, 93-94

DTP

- disabling*, 94
- trunking mode characteristics*, 95

encapsulation method, specifying, 95-96

removing VLANs from trunk links, 96-97
 scaling, 21
 verifying VLAN port assignments, 97
 VTP

changing modes, 100-101
changing versions, 102
configuring, 98-99
example configuration, 103-104
pruning, 101-102
server mode, 99
setting passwords, 99-100
verifying operation, 102

tuning ingress port queues, 231-233

U

UDLD, 115

undelete command, 38

unicast broadcast floods, controlling, 169

upgrades, performing FSUs, 138-139

uplink failure of switched networks, 18

user Exec mode, 2

user interface features (Cisco IOS), 3

user modes, Cisco IOS Software, 2

user-level passwords, configuring, 30

UTC (coordinated universal time), 47

V

VACLs, 176

configuring, 176-178

example, 178-180

verifying configuration, 178

verifying

broadcast suppression, 170

DHCP snooping configuration, 190

Layer 3 EtherChannel configuration, 76-77

Layer 3 Ethernet interface configuration, 73

port security configuration, 175, 188

private VLAN operation, 107

protocol filtering configuration, 171

routing table configuration, 86

STP operation, 127-130

VACL configuration, 178

virtual interface configuration, 84

VLAN port assignment, 93, 97

VTP operation, 102

WAN interface configuration, 81

versions of VTP, switching, 102

viewing

file system devices, 36-38

firewall load balancing information, 164

IGMP snooping information, 145

installed modules, 34

logging information, 198

power management information, 214

QoS information, 245

SLB information, 157

SNMP information, 206

SPAN information, 211-213

STP information, 120

virtual interfaces

example configuration, 84-85

subinterfaces, configuring, 83-84

verifying configuration, 84

VLAN interfaces, configuring, 82

vlan allocation policy command, 89

VLANs

creating, 88-91

Ethernet, configurable parameters, 88

extended range, creating, 89-90

interfaces, configuring, 82

port assignment, verifying, 93

ports

- dynamic assignment, 91-93*
- static assignment, 91*

private edge VLANs, configuring, 106-107

private VLANs

- configuring, 105-106*
- example configuration, 107-109*
- verifying operation, 107*

removing from trunk links, 96-97

standard range, creating, 89

trunking. *See* trunks

VTP

- changing versions, 102*
- configuring, 88, 98-99*
- example configuration, 103-104*
- modes, 100-101*
- pruning, 101-102*
- server mode, 99*
- setting passwords, 99-100*
- verifying operation, 102*

voice control protocols, SCCP, 255-256

voice ports

- displaying information, 253
- IP phone support, configuring, 250-253
- powered devices, inline power, 249

voice QoS, 254-255

- access layer, configuring, 256-259
- core layer, configuring, 259
- distribution layer, configuring, 259-261
- example, 261

VSL (Virtual Switch Links), 17

VSS (Virtual Switching System), 16

VTP (VLAN Trunking Protocol), 21

- configuring, 88, 98-99
- domain name, specifying, 88
- domain names, 99
- example configuration, 103-104
- modes, 100-101
- pruning, 101-102
- server mode, 99
- setting passwords, 99-100
- verifying operation, 102
- versions, changing, 102

vty access, restricting, 183-184

W

WAN interfaces

- configuring, 78
- Enhanced FlexWAN module, configuring, 78-79
- example configuration, 81-82
- POS, configuring, 80
- SIP module, configuring, 79-80
- verifying configuration, 81

Web browser interface, configuring, 8-9

well-known IP multicast addresses, 297-309

well-known IP protocol numbers, 271-281

well-known port numbers, 284-297

weighted least connection SLB, 147

weighted round-robin SLB, 147

X-Y-Z

XOR (exclusive-OR) operation, 62