



## Preface

---

### Audience

This guide is for the networking professional managing the Catalyst 3550 switch, hereafter referred to as the switch or the multilayer switch. Before using this guide, you should have experience working with the Cisco IOS and be familiar with the concepts and terminology of Ethernet and local area networking.

### Purpose

This guide provides the information you need to configure Layer 2 and Layer 3 software features on your switch. The Catalyst 3550 switch is supported by either the standard multilayer software image (SMI) or the enhanced multilayer software image (EMI). The EMI provides a richer set of enterprise-class features, including hardware-based IP unicast and multicast routing, inter-VLAN routing, routed access control lists (ACLs), and the Hot Standby Router Protocol (HSRP). All Catalyst 3550 Gigabit Ethernet switches are shipped with the EMI pre-installed. Catalyst 3550 Fast Ethernet switches are shipped with either the SMI or the EMI pre-installed. After initial deployment, you can order the Enhanced Multilayer Software Image Upgrade kit to upgrade Catalyst 3550 Fast Ethernet switches from running the SMI to the EMI.

This guide provides procedures for using the commands that have been created or changed for use with the Catalyst 3550 switch. It does not provide detailed information about these commands. For detailed information about these commands, refer to the *Catalyst 3550 Multilayer Switch Command Reference* for this release. For information about the standard IOS Release 12.1 commands, refer to the IOS documentation set available from the Cisco.com home page at **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.1** from the Cisco IOS Software drop-down list.

This guide also includes an overview of the Cluster Management Suite (CMS) web-based, switch management interface, which helps you create and manage clusters of switches. This guide does not provide field-level descriptions of the CMS windows nor does it provide the procedures for configuring switches and switch clusters from CMS. For all CMS window descriptions and procedures, refer to the CMS online help, which is integrated with the software image.

This guide does not describe system messages you might encounter or how to install your switch. For more information, refer to the *Catalyst 3550 Multilayer Switch System Message Guide* for this release and to the *Catalyst 3550 Multilayer Switch Hardware Installation Guide*.

# Organization

This guide is organized into these chapters:

[Chapter 1, “Overview,”](#) lists the software features of this release and provides examples of how the switch can be deployed in a network.

[Chapter 2, “Using the Command-Line Interface,”](#) describes how to access the command modes, use the command-line interface (CLI), and describes CLI messages that you might receive. It also describes how to get help, abbreviate commands, use **no** and **default** forms of commands, use command history and editing features, and how to search and filter the output of **show** and **more** commands.

[Chapter 3, “Getting Started with CMS,”](#) describes the Cluster Management Suite (CMS) web-based, switch management interface. For information on configuring your web browser and accessing CMS, refer to the release notes. For field-level descriptions of all CMS windows and procedures for using the CMS windows, refer to the online help.

[Chapter 4, “Assigning the Switch IP Address and Default Gateway,”](#) describes how to create the initial switch configuration (for example, assign the switch IP address and default gateway information) by using a variety of automatic and manual methods. It also describes how to modify the switch startup configuration.

[Chapter 5, “Clustering Switches,”](#) describes switch clusters and the considerations for creating and maintaining them. The online help provides the CMS procedures for configuring switch clusters. Configuring switch clusters is most easily performed through CMS; therefore, CLI procedures are not provided. Cluster commands are described in the *Catalyst 3550 Multilayer Switch Command Reference*.

[Chapter 6, “Administering the Switch,”](#) describes how to perform one-time operations to administer your switch. It describes how to prevent unauthorized access to your switch through the use of passwords, privilege levels, the Terminal Access Controller Access Control System Plus (TACACS+), and the Remote Authentication Dial-In User Service (RADIUS). It also describes how to set the system date and time, system name and prompt, create a login banner, how to manage the MAC address table, and how to optimize system resources for user-selected features.

[Chapter 7, “Configuring 802.1X Port-Based Authentication,”](#) describes how to configure 802.1X port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. As LANs extend to hotels, airports, and corporate lobbies, insecure environments could be created.

[Chapter 8, “Configuring Interface Characteristics,”](#) defines the types of Layer 2 and Layer 3 interfaces on the switch. It describes the **interface** command and provides procedures for configuring physical interfaces.

[Chapter 9, “Creating and Maintaining VLANs,”](#) describes how to create and maintain VLANs. It includes information about VLAN modes, the VLAN Trunking Protocol (VTP) database, and the VLAN Membership Policy Server (VMPS).

[Chapter 10, “Configuring STP,”](#) describes how to configure basic and advanced spanning-tree features.

[Chapter 11, “Configuring IGMP Snooping and MVR,”](#) describes how to configure Layer 2 Internet Group Management Protocol (IGMP) snooping. It also describes Multicast VLAN Registration (MVR), a local IGMP snooping feature available on the switch, and how to use IGMP filtering to control multicast group membership.

[Chapter 12, “Configuring Port-Based Traffic Control,”](#) describes how to reduce traffic storms by setting broadcast, multicast, and unicast storm-control threshold levels; how to protect ports from receiving traffic from other ports on a switch; how to block unknown broadcast and unicast traffic; and how to configure port security using secure MAC addresses.

[Chapter 13, “Configuring CDP,”](#) describes how to configure Cisco Discovery Protocol (CDP) on your switch.

[Chapter 14, “Configuring UDLD,”](#) describes how to configure the UniDirectional Link Detection (UDLD) feature. UDLD enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists.

[Chapter 15, “Configuring SPAN,”](#) describes how to configure Switch Port Analyzer (SPAN), which selects network traffic for analysis by a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN mirrors traffic received or sent (or both) on a source port, or traffic received on one or more source ports or source VLANs, to a destination port.

[Chapter 16, “Configuring RMON,”](#) describes how to configure remote monitoring (RMON). The RMON feature, which is used with the Simple Network Management Protocol (SNMP) agent in the switch, means that you can monitor all the traffic flowing among switches on all connected LAN segments.

[Chapter 17, “Configuring System Message Logging,”](#) describes how to configure system message logging. It describes the message format, how to change the message display destination device, limit the type of messages sent, configure UNIX server syslog daemon and define the UNIX system logging facility, and timestamp messages.

[Chapter 18, “Configuring SNMP,”](#) describes how to configure the Simple Network Management Protocol (SNMP). It describes how to configure community strings, enable trap managers and traps, set the agent contact and location information, and how to limit TFTP servers used through SNMP.

[Chapter 19, “Configuring Network Security with ACLs,”](#) describes how to configure network security on your switch using two types of access control lists (ACLs), router ACLs and VLAN maps. It describes how to apply ACLs to interfaces and provides examples.

[Chapter 20, “Configuring QoS,”](#) describes how to configure quality of service (QoS) on your switch. With this feature, you can provide preferential treatment to certain types traffic.

[Chapter 21, “Configuring EtherChannel,”](#) describes how to bundle a set of individual ports into a single logical link on Layer 2 and Layer 3 interfaces.

[Chapter 22, “Configuring IP Unicast Routing,”](#) describes how to configuring IP unicast routing on your switch, including configuring IP addressing features, Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF) protocol, and Enhanced IGRP (EIGRP). To use this feature, you must have the enhanced multilayer software image installed on your switch.

[Chapter 23, “Configuring HSRP,”](#) describes how to use Hot Standby Router Protocol (HSRP) to provide routing redundancy for routing IP traffic without depending on the availability of any single router. To use this feature, you must have the enhanced multilayer software image installed on your switch.

[Chapter 24, “Configuring IP Multicast Routing,”](#) how to configuring IP multicast routing. It describes how to use and configure the Internet Group Management Protocol (IGMP), Protocol-Independent Multicast (PIM) protocol, Cisco Group Management Protocol (CGMP) server functionality, and how to inter-operate between PIM and Distance Vector Multicast Routing Protocol (DVMRP) domains. To use this feature, you must have the enhanced multilayer software image installed on your switch.

[Chapter 25, “Configuring MSDP,”](#) describes how to configure the Multicast Source Discovery Protocol (MSDP), which is a mechanism to connect multiple PIM sparse-mode domains. To use this feature, you must have the enhanced multilayer software image installed on your switch.

[Chapter 26, “Configuring Fallback Bridging,”](#) describes how to configure fallback bridging on your switch. With fallback bridging, you can bridge non-IP protocols between VLAN bridge domains and routed ports. To use this feature, you must have the enhanced multilayer software image installed on your switch

[Chapter 27, “Troubleshooting,”](#) describes how to identify and resolve software problems related to the IOS software.

[Appendix A, “Supported MIBs,”](#) lists the supported MIBs for this release and how to use FTP to access the MIB files.

[Appendix B, “Working with the IOS File System, Configuration Files, and Software Images,”](#) describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

[Appendix C, “Unsupported CLI Commands in Release 12.1\(8\)EA1,”](#) lists the unsupported command-line interface (CLI) commands that are displayed when you enter the question mark (?) at the switch prompt. The unsupported commands are listed by software feature and command mode.

## Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ( { } ) group required choices, and vertical bars ( | ) separate the alternative elements.
- Braces and vertical bars within square brackets ( [ { | } ] ) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (<>).

Notes, cautions, and timesavers use these conventions and symbols:



### Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.



### Caution

Means *reader be careful*. In this situation, you might do something that could result equipment damage or loss of data.



### Timesaver

Means the following *will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

## Related Publications

These documents provide complete information about the switch and are available from this Cisco.com site:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/index.htm>

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the “[Ordering Documentation](#)” section on page xxxii.

- *Release Notes for the Catalyst 3550 Multilayer Switch* (not orderable but available on Cisco.com)



### Note

---

Switch requirements and procedures for initial configurations and software upgrades tend to change and therefore appear only in the release notes. Before installing, configuring, or upgrading the switch, refer to the release notes on Cisco.com for the latest information.

---

- *Catalyst 3550 Multilayer Switch Software Configuration Guide* (order number DOC-7811194=)
- *Catalyst 3550 Multilayer Switch Command Reference* (order number DOC-7811195=)
- *Catalyst 3550 Multilayer Switch System Message Guide* (order number DOC-7811196=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 3550 Multilayer Switch Hardware Installation Guide* (order number DOC-7811358=)
- *1000BASE-T Gigabit Interface Converter Installation Note* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)

## Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can send us your comments by completing the online survey. When you display the document listing for this platform, click **Give Us Your Feedback**. After you display the survey, select the manual that you wish to comment on. Click **Submit** to send your comments to the Cisco documentation group.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.  
Attn: Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.