



Catalyst 6500 Series Switch MSFC Command Reference

Cisco IOS Release 12.1(13)E

Corporate Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 526-4100

Text Part Number: OL-3354-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0303R)

Catalyst 6500 Series Switch MSFC Command Reference Copyright © 2002–2003 Cisco Systems, Inc. All rights reserved.



Preface vii

	Audience vii
	Organization vii
	Related Documentation vii
	Conventions viii
	Obtaining Documentation ix
	Obtaining Technical Assistance x
	Obtaining Additional Publications and Information xii
CHAPTER 1	Command-Line Interface 1-1
	Getting Help 1-1
	How to Find Command Options 1-2
	Using the No and Default Forms of Commands 1-5
	Using the CLI String Search 1-5
	Saving Configuration Changes 1-11
	MSFC CLI 1-11
CHAPTER 2	Catalyst 6500 Series Switch MSFC Commands 2-1
	clear ip auth-proxy watch-list 2-2
	config-register 2-3
	config-sync 2-4
	define interface-range 2-5
	high-availability 2-6
	interface range 2-8
	ip address 2-10
	ip auth-proxy max-login-attempts 2-12
	ip auth-proxy watch-list 2-13
	ip local-proxy-arp 2-15
	ip multicast rpf backoff 2-16
	ip multicast rpf interval 2-18
	ip verify unicast source reachable-via 2-19
	ip wccp redirect 2-21
	ip wccp redirect 2-21

ipx network 2-23 maximum-paths 2-27 mls aclmerge algorithm 2-28 mls ip 2-30 mls ip cef load-sharing full 2-31 mls ip cef rate-limit 2-32 mls ip delete-threshold 2-34 mls ip inspect 2-35 mls ip install-threshold 2-36 mls ip multicast consistency-check 2-37 mls ip multicast stub 2-39 mtu 2-40 redundancy 2-42 set traffic-index 2-43 show fm features 2-44 show fm inband-counters 2-46 show fm insp 2-47 show fm interface 2-48 show fm reflexive 2-50 show fm summary 2-51 show fm vlan 2-52 show ip auth-proxy watch-list 2-54 show ip wccp web-cache detail 2-55 show I3-mgr 2-57 show microcode 2-59 show msfc2 rom-monitor 2-60 show redundancy 2-61 show scp 2-62 show slot0: 2-64 show standby delay 2-67 snmp-server enable traps 2-68 standby delay minimum reload 2-71 standby ip 2-73 standby track 2-75 upgrade rom-monitor 2-77

APPENDIX A ACTONYMS A-1

APPENDIX B Acknowledgments for Open-Source Software B-1

INDEX

1



Preface

This preface describes the audience, organization, and conventions of this publication, and provides information on how to obtain related documentation.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst 6500 series switches.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Command-Line Interface	Describes the Multilayer Switching Feature Card command-line interface.
Chapter 2	Catalyst 6500 Series Switch MSFC Commands	Lists alphabetically and provides detailed information for MSFC-specific commands.
Appendix A	Acronyms	Defines the acronyms used in this publication.

Related Documentation

The Catalyst 6500 series switch Cisco IOS documentation set includes these documents:

- Catalyst 6500 Series Switch Module Installation Guide
- Catalyst 6500 Series Switch IOS Software Configuration Guide
- Catalyst 6500 Series Switch IOS System Message Guide
- Release Notes for Catalyst 6500 Series Switch IOS Software Release X.X

The Cisco IOS documentation set includes these documents:

- Configuration Fundamentals Configuration Guide
- Command Reference

For information about MIBs, refer to this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface .
italic font	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars. Braces can also be used to group keywords and/or aguments; for example, { interface <i>interface</i> type }.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in <i>italic screen</i> font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:



Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:



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

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

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 may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

• Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

http://www.cisco.com/en/US/partner/ordering/index.shtml

 Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems Attn: Customer Document Ordering 170 West Tasman Drive San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- 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

To obtain customized information and service, you can self-register on Cisco.com at this URL: http://tools.cisco.com/RPF/register/register.do

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: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business
 operations remain functional. You and Cisco are willing to commit resources during normal
 business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require 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 this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

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

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

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

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

• The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

• Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

http://www.ciscopress.com

• *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

http://www.cisco.com/go/packet

• iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

http://www.cisco.com/go/iqmagazine

• Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

• Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html



Command-Line Interface

This chapter provides information for understanding and using the Catalyst 6500 series switch Cisco IOS software using the command-line interface (CLI). This chapter includes the following sections:

- Getting Help, page 1-1
- How to Find Command Options, page 1-2
- MSFC CLI, page 1-11

For an overview of the Catalyst 6500 series switch Cisco IOS software configuration, refer to the *Catalyst 6500 Series IOS Software Configuration Guide*.

Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark (?) at the system prompt. You also can obtain a list of any command's associated keywords and arguments with the context-sensitive help feature.

Table 1-1 lists commands you can enter to get help that is specific to a command mode, a command, a keyword, or an argument.

Command	Purpose
abbreviated-command-entry?	Obtain a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.)
abbreviated-command-entry <tab></tab>	Complete a partial command name.
?	List all commands available for a particular command mode.
command ?	List a command's associated keywords. Leave a space between the command and question mark.
command keyword ?	List a keyword's associated arguments. Leave a space between the keyword and question mark.

Table 1-1 Getting Help

How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords. To display keywords for a command, enter a question mark (?) at the configuration prompt or after entering part of a command followed by a space. The Catalyst 6500 series switch software displays a list of available keywords along with a brief description of the keywords. For example, if you are in global configuration mode and want to see all the keywords for the **arap** command, you enter **arap**?

Table 1-2 shows examples of how you can use the question mark (?) to assist you in entering commands and also guides you through entering the following commands:

- interface gigabitethernet 1/1
- channel-group 1 mode auto

Table 1-2 How to Find Command Options

Command	Comment
Router> enable Password: <password> Router#</password>	Enter the enable command and password to access privileged EXEC commands.
	You are in privileged EXEC mode when the prompt changes to Router#.
Router# configure terminal	Enter global configuration mode.
<pre>Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	You are in global configuration mode when the prompt changes to Router(config)#.
<pre>Router(config)# interface gigabitethernet ? <1-9> GigabitEthernet interface number Router(config)# interface gigabitethernet 1/1 Router(config-if)#</pre>	Enter interface configuration mode by specifying the Gigabit Ethernet interface that you want to configure using the interface gigabitethernet global configuration command.
	Enter a ? to display what you must enter next on the command line. In this example, you must enter an interface number from 1 to 9 in the format <i>module-number/port-number</i> .
	You are in interface configuration mode when the prompt changes to Router(config-if)#.

Command		Comment	
Router(config-if)#?		Enter a ? to display a list of all the	
Interface configurat	ion commands:	interface configuration commands	
access-expression	Build a bridge boolean access expression	•	
apollo	Apollo interface subcommands	available for the Gigabit Ethernet	
appletalk	Appletalk interface subcommands	interface.	
arp	Set arp type (arpa, probe, snap) or timeout		
backup	Modify backup parameters		
bandwidth	Set bandwidth informational parameter		
bgp-policy	Apply policy propogated by bgp community string		
bridge-group	Transparent bridging interface parameters		
carrier-delay	Specify delay for interface transitions		
cdp	CDP interface subcommands		
channel-group	Etherchannel/port bundling configuration		
clns	CLNS interface subcommands		
	OSI CMNS		
cmns			
	Assign a custom queue list to an interface		
decnet	Interface DECnet config commands		
default	Set a command to its defaults		
delay	Specify interface throughput delay		
description	Interface specific description		
dlsw	DLSw interface subcommands		
dspu	Down Stream PU		
exit	Exit from interface configuration mode		
fair-queue	Enable Fair Queuing on an Interface		
flowcontrol	Configure flow operation.		
fras	DLC Switch Interface Command		
help	Description of the interactive help system		
hold-queue	Set hold queue depth		
ip	Interface Internet Protocol config commands		
ipx	Novell/IPX interface subcommands		
isis	IS-IS commands		
iso-igrp	ISO-IGRP interface subcommands		
•			
Doutor (config if)#			
Router(config-if)# Router(config-if)# c	hannel_group 2	Enter the command that you want to	
	oup of the interface	configure for the controller. In this	
		example, the channel-group	
Router(config-if)#ch	annel-group		
		command is used.	
		Enter a ? to display what you must	
		enter next on the command line. In	
		this example, you must enter the	
		group keyword.	
		Because a <cr>> is not displayed, it</cr>	
		indicates that you must enter more	
		information to complete the command.	

Table 1-2How to Find Command Options (continued)

Command	Comment
Router(config-if)# channel-group ? <1-256> Channel group number Router(config-if)#channel-group	After you enter the group keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter a channel group number from 1 to 256.
	Because a <cr>> is not displayed, it indicates that you must enter more information to complete the command.</cr>
<pre>Router(config-if)# channel-group 1 ? mode Etherchannel Mode of the interface Router(config-if)#</pre>	After you enter the channel group number, enter a ? to display what you must enter next on the command line. In this example, you must enter the mode keyword.
	Because a <cr>> is not displayed, it indicates that you must enter more information to complete the command.</cr>
Router(config-if)# channel-group 1 mode ? auto Enable PAgP only if a PAgP device is detected desirable Enable PAgP unconditionally on Enable Etherchannel only Router(config-if)#	After you enter the mode keyword, enter a ? to display what you must enter next on the command line. In this example, you must enter the auto , desirable , or on keyword.
	Because a <cr>> is not displayed, it indicates that you must enter more information to complete the command.</cr>
<pre>Router(config-if)# channel-group 1 mode auto ?</pre>	In this example, the auto keyword is entered. After you enter the auto keyword, enter a ? to display what you must enter next on the command line.
	Because a <cr>> is displayed, it indicates that you can press Return to complete the command. If additional keywords are listed, you can enter more keywords or press Return to complete the command.</cr>
Router(config-if)# channel-group 1 mode auto Router(config-if)#	In this example, press Return to complete the command.

Using the No and Default Forms of Commands

Almost every configuration command has a **no** form. In general, enter the **no** form to disable a function. Use the command without the keyword **no** to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, specify the **no ip routing** command and specify **ip routing** to reenable it. This publication provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

Configuration commands can have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets variables to their default values. This publication describes what the **default** form of a command does if the command is not the same as the **no** form.

Using the CLI String Search

The pattern in the command output is referred to as a string. The CLI string search feature allows you to search or filter any **show** or **more** command output and allows you to search and filter at --More-- prompts. This feature is useful when you need to sort though large amounts of output, or if you want to exclude output that you do not need to see.

With the search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can then specify a maximum of one filter per command or start a new search from the --More-- prompt.

A regular expression is a pattern (a phrase, number, or more complex pattern) software uses to match against **show** or **more** command output. Regular expressions are case sensitive and allow for complex matching requirements. Examples of simple regular expressions are Serial, misses, and 138. Examples of complex regular expressions are 00210..., (is), and [Oo]utput.

You can perform three types of filtering:

- Use the **begin** keyword to begin output with the line that contains a specified regular expression.
- Use the include keyword to include output lines that contain a specified regular expression.
- Use the **exclude** keyword to exclude output lines that contain a specified regular expression.

You can then search this filtered output at the --More-- prompts.



The CLI string search function does not allow you to search or filter backward through previous output; filtering cannot be specified using HTTP access to the CLI.

Regular Expressions

A regular expression can be a single character that matches the same single character in the command output or multiple characters that match the same multiple characters in the command output. This section describes how to create both single-character patterns and multiple-character patterns and how to create more complex regular expressions using multipliers, alternation, anchoring, and parentheses.

Single-Character Patterns

The simplest regular expression is a single character that matches the same single character in the command output. You can use any letter (A-Z, a-z) or digit (0-9) as a single-character pattern. You can also use other keyboard characters (such as ! or \sim) as single-character patterns, but certain keyboard characters have special meaning when used in regular expressions. Table 1-3 lists the keyboard characters with special meaning.

Character	Special Meaning
	Matches any single character, including white space.
*	Matches 0 or more sequences of the pattern.
+	Matches 1 or more sequences of the pattern.
?	Matches 0 or 1 occurrences of the pattern.
٨	Matches the beginning of the string.
\$	Matches the end of the string.
_ (underscore)	Matches a comma (,), left brace ({), right brace (}), left parenthesis ((), right parenthesis ()), the beginning of the string, the end of the string, or a space.

 Table 1-3
 Characters with Special Meaning

To enter these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\). These examples are single-character patterns matching a dollar sign, an underscore, and a plus sign, respectively.

\\$ _ \+

You can specify a range of single-character patterns to match against command output. For example, you can create a regular expression that matches a string containing one of the following letters: a, e, i, o, or u. One and only one of these characters must exist in the string for pattern matching to succeed. To specify a range of single-character patterns, enclose the single-character patterns in square brackets ([]). For example,

[aeiou]

matches any one of the five vowels of the lowercase alphabet, while

[abcdABCD]

matches any one of the first four letters of the lower- or uppercase alphabet.

You can simplify ranges by entering only the end points of the range separated by a dash (-). Simplify the previous range as follows:

[a-dA-D]

To add a dash as a single-character pattern in your range, include another dash and precede it with a backslash:

[a-dA-D\-]

You can also include a right square bracket (]) as a single-character pattern in your range. To do so, enter the following:

[a-dA-D\-\]]

The previous example matches any one of the first four letters of the lower- or uppercase alphabet, a dash, or a right square bracket.

You can reverse the matching of the range by including a caret ($^{\wedge}$) at the start of the range. This example matches any letter except the ones listed:

[^a-dqsv]

This example matches anything except a right square bracket (]) or the letter d:

[^\]d]

Multiple-Character Patterns

When creating regular expressions, you can also specify a pattern containing multiple characters. You create multiple-character regular expressions by joining letters, digits, or keyboard characters that do not have special meaning. For example, a4% is a multiple-character regular expression. Put a backslash in front of the keyboard characters that have special meaning when you want to remove their special meaning.

With multiple-character patterns, order is important. The regular expression a4% matches the character a followed by a 4 followed by a % sign. If the string does not have a4%, in that order, pattern matching fails. This multiple-character regular expression

a.

uses the special meaning of the period character to match the letter a followed by any single character. With this example, the strings ab, a!, or a2 are all valid matches for the regular expression.

You can remove the special meaning of the period character by putting a backslash in front of it. In the following expression

a∖.

only the string a. matches this regular expression.

You can create a multiple-character regular expression containing all letters, all digits, all keyboard characters, or a combination of letters, digits, and other keyboard characters. These examples are all valid regular expressions:

telebit 3107 v32bis

Multipliers

You can create more complex regular expressions to match multiple occurrences of a specified regular expression by using some special characters with your single- and multiple-character patterns. Table 1-4 lists the special characters that specify "multiples" of a regular expression.

Character	Description
*	Matches 0 or more single- or multiple-character patterns.
+	Matches 1 or more single- or multiple-character patterns.
?	Matches 0 or 1 occurrences of the single- or multiple-character patterns.

This example matches any number of occurrences of the letter a, including none: **a***

This pattern requires that at least one letter a in the string is matched:

a+

This pattern matches the string bb or bab:

ba?b

This string matches any number of asterisks (*):

**

To use multipliers with multiple-character patterns, you enclose the pattern in parentheses. In the following example, the pattern matches any number of the multiple-character string ab:

(ab)*

As a more complex example, this pattern matches one or more instances of alphanumeric pairs (but not none; that is, an empty string is not a match):

([A-Za-z][0-9])+

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression matches A9b3, but not 9Ab3 because the letters are specified before the numbers.

Alternation

Alternation allows you to specify alternative patterns to match against a string. You separate the alternative patterns with a vertical bar (|). Exactly one of the alternatives can match the string. For example, the regular expression

codex | telebit

matches the string codex or the string telebit, but not both codex and telebit.

Anchoring

You can match a regular expression pattern against the beginning or the end of the string. That is, you can specify that the beginning or end of a string contains a specific pattern. You "anchor" these regular expressions to a portion of the string using the special characters shown in Table 1-5.

Table 1-5 Special Characters Used for Anchoring

Character	Description	
٨	Matches the beginning of the string.	
\$	Matches the end of the string.	

This regular expression matches a string only if the string starts with abcd:

^abcd

In contrast, this expression is in a range that matches any single letter, as long as it is not the letters a, b, c, or d:

[^abcd]

With this example, the regular expression matches a string that ends with .12:

\$\.12

Contrast these anchoring characters with the special character underscore (_). The underscore matches the beginning of a string (^), the end of a string (\$), parentheses (), space (), braces {}, comma (,), or underscore (_). With the underscore character, you can specify that a pattern exist anywhere in the string.

For example:

1300

matches any string that has 1300 somewhere in the string. The string's 1300 can be preceded by or end with a space, brace, comma, or underscore. For example:

{1300_

matches the regular expression, but 21300 and 13000 do not.

Using the underscore character, you can replace long regular expression lists, such as the following:

^1300\$ ^1300(space) (space)1300 {1300, ,1300, {1300} ,1300, (1300

with

1300

Parentheses for Recall

As shown in the "Multipliers" section on page 1-7, you use parentheses with multiple-character regular expressions to multiply the occurrence of a pattern. You can also use parentheses around a single- or multiple-character pattern to remember a pattern for use elsewhere in the regular expression.

To create a regular expression that recalls a previous pattern, you use parentheses to indicate a remembered specific pattern and a backslash (\) followed by an integer to reuse the remembered pattern. The integer specifies the occurrence of the parentheses in the regular expression pattern. If you have more than one remembered pattern in your regular expression, then 1 indicates the first remembered pattern, 2 indicates the second remembered pattern, and so on.

This regular expression uses parentheses for recall:

a(.)bc(.) |1|2

This regular expression matches an a followed by any character (call it character 1), followed by bc followed by any character (character 2), followed by character 1 again, followed by character 2 again. The regular expression can match aZbcTZT. The software remembers that character 1 is Z and character 2 is T and then uses Z and T again later in the regular expression.

alt Keyword Usage

When you enable high-availability redundancy, every configuration command executed on the designated MSFC is sent to the nondesignated MSFC. Also, the running configuration synchronization is updated when you enter the **copy** *source* **running-config** command on the designated MSFC.

The two states for the configuration synchronization are as follows:

- Config Sync AdminStatus—Signifies what the user has configured for this feature at that moment
- Config Sync RuntimeStatus—Enabled only when the following occurs:
 - The Config Sync AdminStatus is enabled on both the designated and nondesignated MSFCs
 - The designated and nondesignated MSFCs are running compatible images

To configure both MSFCs from a single console, enter the **alt** keyword to specify an alternate configuration. When specifying the alternate configuration, the configuration that is specified before the **alt** keyword relates to the MSFC on the supervisor engine in slot 1 of the switch; the configuration that is specified after the **alt** keyword relates to the MSFC on the SUPERVISOR engine in slot 2.



You must enter the alt keyword when you enable Config Sync AdminStatus.

When you enable the Config Sync RuntimeStatus, the following occurs:

- No configuration mode is available on the CLI of the nondesignated MSFC; EXEC mode is available. Configuration of both MSFCs is made through the console or a Telnet session on the designated MSFC.
- The **alt** keyword is available and required (see the "alt Keyword Usage" section on page 1-9 for more information on the **alt** keyword)
- The running and startup configurations are synchronized

When the Config Sync RuntimeStatus is in disabled mode, the following occurs:

- Configuration mode is available on the CLI of both MSFCs
- The alt keyword is available but optional
- The running and startup configurations are not synchronized

Table 1-6 shows the interface and global configuration commands that contain the **alt** keyword:

Table 1-6	Interface and Global	Configuration Commands	Containing the alt Keyword

Interface Configuration Commands	Global Configuration Commands
 [no] standby [group_number] ip [ip_address [secondary]] alt [no] standby [group_number] ip [ip_address [secondary]] [no] standby [group_number] priority priority [preempt [delay delay]] alt [no] standby [group_number] priority priority [preempt [delay delay]] [no] ip address ip_address mask [secondary] alt [no] ip address ip_address mask [secondary] 	 [no] hostname hostname alt hostname hostname [no] ip default-gateway ip_address alt [no] ip default-gateway ip_address router bgp autonomous_system bgp router-id ip_address [alt ip_address] router ospf process_id router-id ip_address [alt ip_address]
 [no] ipx network network [encapsulation encapsulation_type [secondary]] [alt [no] ipx network network [encapsulation encapsulation_type [secondary]]] 	

This example shows how the **alt** keyword is used when entering the **ip address** command:

Router-1(config-if)# ip address 1.2.3.4 255.255.255.0 alt ip address 1.2.3.5 255.255.255.0

Saving Configuration Changes

To save your configuration changes to your startup configuration so that they will not be lost if there is a system reload or power outage, enter the following command:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

[OK] Router#

On most platforms, this step saves the configuration to NVRAM. On the Class A Flash file system platforms, this step saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE environment variable defaults to NVRAM.

MSFC CLI

You can access the Multilayer Switch Feature Card (MSFC) command-line interface (CLI) by entering commands from the supervisor engine CLI. These sections describe the MSFC CLI:

- Accessing the MSFC CLI from the Supervisor Engine CLI, page 1-11
- Cisco IOS Command Modes, page 1-12
- Cisco IOS Command-Line Interface, page 1-14

Accessing the MSFC CLI from the Supervisor Engine CLI

These sections describe how to access the MSFC CLI from a directly connected console port or from a Telnet session:

- Accessing the MSFC CLI from the Console Port, page 1-11
- Accessing the MSFC CLI from a Telnet Session, page 1-12

Accessing the MSFC CLI from the Console Port

You can enter the **switch console** command to access the MSFC CLI from the supervisor engine CLI directly connected to the console port. To exit from the MSFC CLI and return to the supervisor engine CLI, enter $^CC^C$ at the Router> prompt.

To access the MSFC CLI from the supervisor engine CLI, perform this task:

Task	Command
Access the MSFC CLI from the supervisor engine CLI.	switch console [mod] ¹

1. The *mod* variable specifies the module number of the MSFC; either 15 (if the MSFC is installed on the supervisor engine in slot 1) or 16 (if the MSFC is installed on the supervisor engine in slot 2). If no module number is specified, the console will switch to the MSFC on the active supervisor engine.



To access the MSFC CLI on the standby MSFC, connect to the console port of the standby supervisor engine.

This example shows how to access the active MSFC CLI from the active supervisor engine CLI, and how to exit the MSFC CLI and return to the supervisor engine CLI:

```
Console> (enable) switch console 15
Trying Router-15...
Connected to Router-15.
Type ^C^C^C to switch back...
Router>^C^C^C
Console> (enable)
```

Accessing the MSFC CLI from a Telnet Session

You can enter the **session** *mod* command to access the MSFC CLI from the supervisor engine CLI using a Telnet session. To exit from the MSFC CLI back to the supervisor engine CLI, enter the **exit** command at the Router> prompt.

Note

The supervisor engine software sees the MSFC as module 15 (when installed on a supervisor engine in slot 1) or module 16 (when installed on a supervisor engine in slot 2).

This example shows how to access the MSFC from the supervisor engine CLI, and how to exit the MSFC CLI and return to the supervisor engine CLI:

Console> (enable) **session 15** Router> **exit** Console> (enable)

Note

In addition to the methods described in the "Accessing the MSFC CLI from the Supervisor Engine CLI" section on page 1-11, you can configure Cisco IOS software to support direct Telnet access to the MSFC. Refer to "Configuring Authentication" in the *Cisco IOS Security Configuration Guide* at this URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt1/scdathen. htm

Cisco IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. To get a list of the commands in a given mode, type a question mark (?) at the system prompt. For more information, see the "Getting a List of Cisco IOS Commands and Syntax" section on page 2-14.

When you start a session on the supervisor engine, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in EXEC mode. To have access to all commands, you must enter privileged EXEC mode. Normally, you must type in a password to access privileged EXEC mode. From privileged EXEC mode, you can type in any EXEC command or access global configuration mode. Most of the EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The EXEC commands are not saved across reboots of the supervisor engine.

The configuration modes allow you to make changes to the running configuration. If you later save the configuration, these commands are stored across supervisor engine reboots. You must start at global configuration mode. From global configuration mode, you can enter interface configuration mode, subinterface configuration mode, and a variety of protocol-specific modes.

ROM monitor mode is a separate mode used when the supervisor engine cannot boot properly. For example, the supervisor engine might enter ROM monitor mode if it does not find a valid system image when it is booting, or if its configuration file is corrupted at startup. For more information, see the *"Catalyst 6500 Series IOS Command Reference."*

Table 1-7 lists and describes the most commonly used Cisco IOS modes.

Mode	Description of Use	How to Access	Prompt
User EXEC	Connect to remote devices, change terminal settings on a temporary basis, perform basic tests, and display system information.	Log in.	Router>
Privileged EXEC (enable)	Set operating parameters. The privileged command set includes the commands in user EXEC mode as well as the configure command. Use this command to access the other command modes.	From the user EXEC mode, enter the enable command and the enable password.	Router#
Global configuration Configure features that affect the system as a whole.		From the privileged EXEC mode, enter the configure terminal command.	Router(config)#
Interface configuration Many features are enabled for a particular interface. Interface commands enable or modify the operation of a Gigabit Ethernet or Fast Ethernet interface.		From global configuration mode, enter the interface <i>type</i> <i>location</i> command.	Router(config-if)#
Console configuration	From the directly connected console or the virtual terminal used with Telnet, use this configuration mode to configure the console interface.	From global configuration mode, enter the line console 0 command.	Router(config-line)#

Table 1-7 Frequently Used Cisco IOS Command Modes

The Cisco IOS command interpreter, called the EXEC, interprets and executes the commands that you enter. You can abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the **show** command to **sh** and the **configure terminal** command to **config t**.

When you type **exit**, the MSFC backs out one level. To exit configuration mode completely and return to privileged EXEC mode, press **Ctrl-Z**.

Getting a List of Cisco IOS Commands and Syntax

In any command mode, you can get a list of available commands by entering a question mark (?).

```
Router> ?
```

To obtain a list of commands that begin with a particular character sequence, type in those characters followed by the question mark (?). Do not include a space. This form of help is called word help, because it completes a word for you.

Router# co? configure

To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you have already entered.

```
Router# configure ?

memory Co

network Co

overwrite-network Ov

terminal Co
```

Configure from NV memory Configure from a TFTP network host Overwrite NV memory from TFTP network host Configure from the terminal

To redisplay a command you previously entered, press the up-arrow key or **Ctrl-P**. You can continue to press the up-arrow key to see the last 20 commands that you entered.



If you are having trouble entering a command, check the system prompt, and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

Press **Ctrl-Z** in any mode to immediately return to privileged EXEC mode. Enter **exit** to return to the previous mode.

Cisco IOS Command-Line Interface

These sections describe basic Cisco IOS configuration tasks that you need to understand before you configure routing:

- Accessing Cisco IOS Configuration Mode, page 1-14
- Viewing and Saving the Cisco IOS Configuration, page 1-15
- Bringing Up an MSFC Interface, page 1-15

Accessing Cisco IOS Configuration Mode

To access the Cisco IOS configuration mode, perform this task:



Enter the **switch console** command to access the MSFC CLI from the supervisor engine CLI when directly connected to the supervisor engine console port. To access the MSFC from a Telnet session, see the "Accessing the MSFC CLI from a Telnet Session" section on page 1-12.

Task	Command
If you are in the supervisor engine CLI, enter the MSFC CLI.	Console> switch console [mod_num]
At the EXEC prompt, enter enable mode.	Router> enable
At the privileged EXEC prompt, enter global configuration mode.	Router# configure terminal
Enter the commands to configure routing.	(Refer to the appropriate configuration tasks in the <i>Catalyst</i> 6500 Series IOS Software Configuration Guide.)
Exit configuration mode.	Router(config)# Ctrl-Z

Viewing and Saving the Cisco IOS Configuration

To view and save the configuration after you make changes, perform this task:

	Task	Command
р 1	View the current operating configuration at the privileged EXEC prompt.	Router# show running-config
p 2	View the configuration in NVRAM.	Router# show startup-config
р 3	Save the current configuration to NVRAM.	Router# copy running-config startup-config

Bringing Up an MSFC Interface

In some cases, an MSFC interface might be administratively shut down. You can check the status of an interface using the **show interface** command.

Note

In a redundant supervisor engine setup, if an interface on one MSFC is shut down, the matching VLAN interface on the redundant MSFC will stop forwarding packets. Therefore, you should manually shut down the matching interface on the redundant MSFC.

To bring up an MSFC interface that is administratively shut down, perform this task in privileged mode:

	Task	Command
Step 1	Specify the interface to bring up.	Router(config)# interface <i>interface_type interface_number</i>
Step 2	Bring the interface up.	Router(config-if)# no shutdown
Step 3	Exit configuration mode.	Router(config-if)# Ctrl-Z



Catalyst 6500 Series Switch MSFC Commands

This chapter contains an alphabetical listing of the Multilayer Switching Feature Card (MSFC) commands that support the Cisco IOS software.

The Catalyst 6500 Series Switch MSFC Command Reference—Release 12.1(13)E contains only those commands that are unique to the MSFC. For information about Cisco IOS commands not contained in this publication, refer to the current Cisco IOS documentation including:

- Cisco IOS Release 12.1 Configuration Fundamentals Configuration Guide
- Catalyst 6500 Series Switch Cisco IOS Command Reference

clear ip auth-proxy watch-list

To delete a single watch-list entry or all watch-list entries, use the **clear ip auth-proxy watch-list** command.

clear ip auth-proxy watch-list {*ip-addr* | *}

Syntax Description	ip-addr	Specifies the IP address to be deleted from the watch list.	
	*	Removes all watch-list entries from the watch list.	
Defaults	This command	l has no default settings.	
Command Modes	Privilieged EX	TEC	
Command History	Release	Modification	
	12.1(13)E	This command was introduced on the MSFC.	
Usage Guidelines	watch-list con	ries in the watch list that you suspect are not valid, you can enter the clear ip auth-proxy mand to clear them manually instead of waiting for the watch list expiry-time to expire.	
Examples	This example shows how to delete a single watch-list entry:		
	Router# clear Router#	r ip auth-proxy watch-list 12.0.0.2	
	This example s	shows how to delete all watch-list entries:	
	Router# clear Router#	f ip auth-proxy watch-list *	
Related Commands	ip auth-proxy	max-login-attempts watch-list proxy watch-list	

config-register

To change the configuration register settings, use the **config-register** command.

config-register value

Syntax Description	value	Hexadecimal or decimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted; vaild values are from 0x0 to 0xFFFF (0 to 65535 in decimal).		
Defaults		ocumentation for your platform for the default configuration register value. For many is, the default is 0x2102, which causes the router to boot from Flash memory and the e ignored.		
Command Modes	Global configu	ration		
Command History	Release	Modification		
-	12.1E	This command was introduced on the MSFC.		
Usage Guidelines	This command applies only to platforms that use a software configuration register. The lowest four bits of the configuration register (bits 3, 2, 1, and 0) form the boot field. The boot field determines if the router boots manually, from ROM, or from Flash or the network.			
	To change the boot field value and leave all other bits set to their default values, follow these guidelines:			
	• If you set the configuration register boot field value to 0x0, you must boot the operating system manually with the boot command.			
	• If you set the configuration register boot field value to 0x1, the router boots using the default ROM software.			
	• If you set the configuration register boot field to any value from 0x2 to 0xF, the router uses the boot field value to form a default boot filename for booting from a network server.			
		mation about the configuration register bit settings and default filenames, see the ater hardware installation guide.		
Examples	_	shows how to set the configuration register to boot the system image from Flash memory:		
	Router(Config Router(config	n)# config-register 0x2102 n)#		

config-sync

To enable configuration synchronization, use the **config-sync** command. Use the **no** form of this command to disable configuration synchronization.

config-sync

no config-sync

- Syntax Description This command has no arguments or keywords.
- **Defaults** This command has no default settings.
- Command Modes High-availability redundancy submode

Command History	Release	Modification
	12.1E	This command was introduced on the MSFC.

Examples

This example shows how to enable configuration synchronization:

Router(config)# redundancy
Router(config-r)# high-availability
Router(config-r-ha)# config-sync
Router(config-r-ha)#

This example shows how to disable configuration synchronization:

Router(config)# redundancy
Router(config-r)# high-availability
Router(config-r-ha)# no config-sync
Router(config-r-ha)#

define interface-range

To create an interface-range macro, use the define interface-range command.

define interface-range macro-name interface-range

Syntax Description	macro-name	Name of the interface range macro; the macro name can contain up to 32 characters.	
	interface-range	Interface range; for a list of valid values for interface ranges, see the "Usage Guidelines" section.	
Defaults	This command has	s no default settings.	
Command Modes	Global configurati	on	
Command History	Release	Modification	
	12.1E	This command was introduced on the MSFC.	
Usage Guidelines	The macro name is a 32-character maximum character string.		
-	A macro can contain up to five ranges. An interface range cannot span slots. When entering the <i>interface-range</i> , these formats can be used:		
	• card-type {slot}/{first-interface} - {last-interface}		
	• card-type {slot}/{first-interface} - {last-interface}		
	Valid values for <i>card-type</i> are as follows:		
	• ge-wan		
	• pos		
	• vlan vlan-id (valid values are from 1 to 4094)	
Examples	This example shows how to create a multiple-interface macro:		
	Router(config)# Router(config)#	define interface-range macrol vlan 223, pos 6/1	
Related Commands	interface range		

high-availability

To enable high-availability redundancy and enter the high-availability redundancy submode, use the **high-availability** command.

high-availability

- Syntax Description This command has no arguments or keywords.
- Defaults This command has no default settings.
- Command Modes Redundancy configuration submode

Command History	Release	Modification
	12.1E	This command was introduced on the MSFC.

Usage Guidelines

Once you enter high-availability redundancy configuration submode, these options are available:

[no] config-sync—Enables automatic startup and running-configuration synchronization. Use the **no** form of this command to disable automatic startup and running-configuration synchronization.

When you enable the Config Sync RuntimeStatus, the following occurs:

- No configuration mode is available on the CLI of the nondesignated MSFC; EXEC mode is available
- The alt keyword is available and required (see the "alt Keyword Usage" section on page 1-9 for information on the alt keyword)
- The running and startup configurations are synchronized

When the Config Sync RuntimeStatus is in disabled mode, the following occurs:

- Configuration mode is available on the CLI of both MSFCs
- The alt keyword is available but optional
- The running and startup configurations are not synchronized
- exit—Exits from high-availability configuration mode
- no—Negates a command or set its defaults
- **[no] single-router-mode**—Enters single router mode. Use the **no** form of this command to exit out of single router mode. Once you enter single-router mode, this option is available:
 - failover table-update-delay *time*—Sets the delay in seconds between the switch over detection and the hardware FIB reload. The valid values for *time* are from 0 to 4294967295 seconds.

When you enable high-availability redundancy, every configuration command executed on the designated MSFC is sent to the nondesignated MSFC. Also, the running configuration synchronization is updated when you enter the **copy** *source* **running-config** command on the designated MSFC.

When you enable high-availability redundancy, the configuration mode is disabled on the nondesignated MSFC; only the EXEC mode is available. For example, in the following, Router-16 is the nondesignated MSFC; high-availability redundancy and configuration synchronization are enabled:

Console>(enable) **session 16** Trying Router-16... Connected to Router-16. Escape character is '^]'.

Router-16> **enable** Router-16# **configure terminal** Config mode is disabled on non-designated Router, please configure from designated Router Router-16>

Examples

This example shows how to enable high-availability redundancy and enter the high-availability redundancy submode:

```
Router(config)# redundancy
Router(config-r)# high-availability
Router(config-r-ha)#
```

Related Commands redundancy

show redundancy (See the Catalyst 6500 Series Switch Cisco IOS Command Reference)

interface range

To execute a command on multiple ports at the same time, use the interface range command.

interface range {port-range | macro name}

Syntax Description	port-range	Port range; for a list of valid values for <i>port-range</i> , see the "Usage Guidelines" section.	
	macro name	Specifies the name of a macro.	
Defaults	This command has no default settings.		
Command Modes	Global or interface configuration		
Command History	Release	Modification	
	12.1E	This command was introduced on the MSFC.	
Usage Guidelines	You can use the interface range command on existing VLAN SVIs only. To display VLAN SVIs, enter the show running config command. VLANs not displayed cannot be used in the interface range command.		
	The values entered with the interface range command are applied to all existing VLAN SVIs.		
	Before you can use a macro, you must define a range using the define interface-range command.		
	All configuration changes made to a port range are saved to NVRAM, but port ranges created with the interface range command do not get saved to NVRAM.		
	You can enter the port range in two ways:		
	• Specifying up to five port ranges		
	Specifying a previously defined macro		
	You can either specify the ports or the name of a port range macro. A port range must consist of the same port type, and the ports within a range cannot span slots.		
	You can define up to five port ranges on a single command, with each range separated by a comma.		
	When you define a range, you must enter a white space between the first port and the hyphen (-):		
	When you define a range, you must enter a white space before and after the hyphen (-) as follows:		
	interface range pos 7/1 - 7, pos9/5 - 408		
	If your system is configured with a Supervisor Engine 1, valid values for <i>vlan-id</i> are from 1 to 1005. If your system is configured with a Supervisor Engine 2, valid values for <i>vlan-id</i> are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine 1.		

When entering the *port-range*, these formats can be used:

- card-type {slot}/{first-port} {last-port}
- card-type {slot}/{first-port} {last-port}

Valid values for *card-type* are as follows:

- ge-wan
- pos
- vlan vlan-id

You cannot specify both a macro and an interface range in the same command. After creating a macro, the CLI does not allow you to enter additional ranges. If you have already entered an interface range, the CLI does not allow you to enter a macro.

You can also specify a single interface in port-range.

Examples	This example shows how to execute a command on two port ranges:
	Router(config)# interface range pos 7/1 - 7, pos 9/5 - 408 Router(config-if)#
	This example shows how to execute a port-range macro:
	Router(config)# interface range macro macrol Router(config-if)#

Related Commands define interface-range

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command. Use the **no** form of this command to remove an IP address or disable IP processing..

ip address ip_address mask [secondary]

no ip address *ip_address mask* [**secondary**]

Syntax Description	ip-address	IP address.
	mask	Mask for the associated IP subnet.
	secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
Defaults	No IP address is	s defined for the interface.
Command Modes	Interface config	uration
Command History	Release	Modification
-	12.1E	This command was introduced on the MSFC.
	An interface car by the Cisco IO	ress <i>ip-address mask</i> [secondary] alt [no] ip address <i>ip-address mask</i> [secondary] n have one primary IP address and multiple secondary IP addresses. Packets generated S software always use the primary IP address. Therefore, all routers and access servers nould share the same primary network number.
	Hosts can deter	mine subnet masks using the Internet Control Message Protocol (ICMP) Mask Request rs respond to this request with an ICMP Mask Reply message.
		IP processing on a particular interface by removing its IP address with the no ip address software detects another host using one of its IP addresses, it will print an error message
	Secondary addr other than routir	yword secondary allows you to specify an unlimited number of secondary addresses. esses are treated like primary addresses, except the system never generates datagrams ng updates with secondary source addresses. IP broadcasts and ARP requests are handled interface routes in the IP routing table.
	Secondary IP ac applications:	ldresses can be used in a variety of situations. The following are the most common

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that there are many subnets on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.



If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.



When you are routing Open Shortest Path First (OSPF), ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must do two things:

- Disable IP routing (specify **no ip routing**).
- Add the interface to a bridge group. (See the **bridge-group** command.)

To concurrently route and transparently bridge IP on an interface, see the bridge crb command.

Examples	-	mple, 131.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are for Ethernet interface 0:
	ip address 192.31	: 0 08.1.27 255.255.255.0 7.17 255.255.255.0 secondary 8.17 255.255.255.0 secondary
Related Commands	Command	Description
	bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
	bridge-group	Assigns each network interface to a bridge group.

ip auth-proxy max-login-attempts

To limit the number of login attempts at a firewall interface, use the **ip auth-proxy max-login-attempts** command. Use the **no** form of this command to return to the default setting.

ip auth-proxy max-login-attempts 1-maxint

no ip auth-proxy max-login-attempts

Syntax Description	1-maxint	Specifies the maximum number of login attempts: valid values are from 1 to 2147483647 attempts.
Defaults	<i>1-maxint</i> is 5	
Command Modes	Interface con	figuration
Command History	Release	Modification
-	12.1(13)E	This command was introduced on the MSFC.
Usage Guidelines	The maximum configure the you configure occurs but wi	d is supported on firewall interfaces only. n login attempt functionality is independent of the watch-list feature. If you do not watch-list feature (using the ip access-list hardware permit fragments command) and e the maximum login attempt functionality, the existing authentication proxy behavior th the new number for retries. If you configure the watch-list feature, once the configured empts has been reached, the IP address is put in the watch list.
Examples	•	shows how to set a limit to the number of login attempts at a firewall interface: .g-if) # ip auth-proxy watch-list max-login-attempts 4 .g-if) #
Related Commands	ip access-list <i>Reference</i>) ip auth-prox	-proxy watch-list hardware permit fragments (see the Catalyst 6500 Series Switch Cisco IOS Command y watch-list -proxy watch-list

ip auth-proxy watch-list

To enable and configure the authentication proxy watch list functionality, use the **ip auth-proxy watch-list** command. See the "Usage Guidelines" section for the **no** form of this command usage.

ip auth-proxy watch-list {{**add-item** *ip-addr*} | **enable** | {**expiry-time** *minutes*}}

no ip auth-proxy watch-list [**add-item** *ip-addr*} | **expiry-time**]

Syntax Description	add-item ip-addr	Adds an IP address to the watch list.
Syntax Description	enable	Enables the watch list feature.
	expiry-time minutes	Specifies the duration of time an entry is in the watch list; see the "Usage Guidelines" section for valid values.
Defaults	The defaults are as follo	ws:
	• <i>minutes</i> is 30 minut	es.
		tionality is disabled.
Command Modes	Interface configuration	
Command History	Release Modi	fication
	12.1(13)E This	command was introduced on the MSFC.
Usage Guidelines	2147483647 in decimal)	nutes are from 0 to the largest 32-bit positive number (0x7FFFFFFF or). Setting the <i>minutes</i> to 0 (zero) places the entries in the list permanently. rted on firewall interfaces only.
	Use the no form of this	command to do the following:
	 no ip auth-proxy w 	watch-list—Disables the watch-list functionality.
	 no ip auth-proxy w 	watch-list add-item <i>ip-addr</i> —Removes the IP address from the watch list.
	 no ip auth-proxy w 	vatch-list expiry-time—Returns to the default setting.
		IP addresses that have opened TCP connections to port 80 and have not sent an o new connection are accepted from this type of IP address (to port 80) and the
	The watch-list entry ren	nains in the watch list for the time specified by expiry-time <i>minutes</i> .
	-	atch-list functionality, no entries are put into the watch list, but the sessions ar ED state. The sessions are deleted after 2 minutes by the timer.

ExamplesThis example shows how to enable the authentication proxy watch list functionality:
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#This example shows how to disable the authentication proxy watch list functionality:

Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#

This example shows how to add an IP address to the watch list:

Router(config-if)# ip auth-proxy watch-list add-item 12.0.0.2
Router(config-if)#

This example shows how to set the duration of time an entry is in the watch list:

Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#

Related Commands ip auth-proxy watch-list ip auth-proxy max-login-attempts show ip auth-proxy watch-list

ip local-proxy-arp

To enable the local proxy ARP feature, use the **ip local-proxy-arp** command. Use the **no** form of this command to disable the feature.

ip local-proxy-arp

no ip local-proxy-arp

Syntax Description	This command	has no arguments or keywords.
Defaults	Disabled	
Command Modes	Interface confi	guration
Command History	Release	Modification
	12.1(2)E	Support for this command was introduced on the MSFC.
Usage Guidelines	subnet where r responds to all the subnet. Use directly to the	y ARP feature allows the MSFC to respond to ARP requests for IP addresses within a formally no routing is required. With the local proxy ARP feature enabled, the MSFC ARP requests for IP addresses within the subnet and forwards all traffic between hosts in this feature only on subnets where hosts are intentionally prevented from communicating Catalyst 6500 series switch on which they are connected. s are disabled on interfaces where the local proxy ARP feature is enabled.
Examples	-	shows how to enable the local proxy ARP feature: (-if) # ip local-proxy-arp (-if) #

ip multicast rpf backoff

To set the PIM backoff interval, use the **ip multicast rpf backoff** command. Use the **no** form of this command to return to the default settings.

ip multicast rpf backoff {{*min max*} | **disable**}

no ip multicast rpf backoff

Syntax Description		Initial RPF backoff delay in milliseconds; valid values are from 1 to 65535 milliseconds.
		Maximum RPF backoff delay in milliseconds; valid values are from 1 to 65535 milliseconds.
	disable	Disables triggered RPF check.
Defaults	If triggered	RPF check is enabled, the defaults are as follows:
	• <i>min</i> is 5	0 milliseconds.
	• <i>max</i> is 5	5000 milliseconds.
Command Modes	Global confi	guration
Command History	Release	Modification
	12.1(11b)E	Support for this command was introduced on the MSFC.
Usage Guidelines	using the ip routing table Once trigger routing table backoff perio	t enable the triggered RPF check, PIM periodically polls the routing tables for changes (set multicast rpf interval command). When you enable the triggered RPF check, PIM polls the es when a change in the routing tables occurs. The <i>min</i> argument sets the initial backoff time. red, PIM waits for additional routing table changes. If the <i>min</i> period expires without further e changes, PIM scans for routing changes. If additional routing changes occur during the od, PIM doubles the length of the backoff period. You can set the maximum interval for the koff period with the <i>max</i> argument.
	Use this con	nmand in the following situation:
	You hav	e frequent route changes in your router (for example, on a dial-in router).
		nt to either reduce the maximum RPF-check interval (for faster availability of IP multicast y established routes).
	• You war check.	nt to increase the RPF-check interval to reduce the CPU load that is introduced by the RPF

 Examples
 This example shows how to set the PIM backoff interval in milliseconds:

 Router(config)# ip multicast rpf backoff 100
 Router(config)#

Related Commandsip multicast rpf interval
show ip rpf events (refer to Cisco IOS documentation)

ip multicast rpf interval

To set the RPF consistency-check interval, use the **ip multicast rpf interval** command. Use the **no** form of this command to return to the default setting.

ip multicast rpf interval *interval*

no ip multicast rpf interval

Syntax Description	interval	Interval in seconds between RPF checks; valid values are from 1 to 10 seconds.
Defaults	10 seconds	
Command Modes	Global config	iration
Command History	Release	Modification
	12.1(11b)E	Support for this command was introduced on the MSFC.
Usage Guidelines	The ip multic	ast rfp interval command sets the interval PIM and polls the routing tables for changes.
Examples	This example	shows how to set the RPF check interval in seconds:
	Router(config Router(config	g)# ip multicast rpf interval 5 g)#
Related Commands	ip multicast r	fp backoff

ip verify unicast source reachable-via

To enable and configure RPF checks, use the **ip verify unicast source reachable-via** command. Use the **no** form of this command to disable RPF.

ip verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping] [list]

no ip verify unicast source reachable-via

Syntax Description	rx	Checks that the source address is reachable on the interface that the packet was received.
	any	Checks that the source address is reachable on any path.
	allow-default	(Optional) Checks that the default route matches the source address.
	allow-self-ping	(Optional) Allows the router to ping itself.
	list	(Optional) Access list number; valid values are from 1 to 199 for a standard IP access list number and from 1300 to 2699 for a standard IP expanded access list number.
Defaults	Unicast RPF is di	sabled.
Command Modes	Interface configur	ation
Command History	Release	Modification
	12.1(8a)E	Support for this command was introduced on the MSFC.
Usage Guidelines	-	ides three basic modes:
	"real" interface allow-default	node—A source address needs only to be present in the FIB and reachable through ce; this situation also applies to the ip verify unicast source reachable-via any t command. The exists-only mode requires that a resolved and reachable source esent in the FIB table. The source address must be reachable through a configured
		The source must be reachable through any of the paths. For example, the source has on load balancing.
		source address must be reachable on the arrived interface. For example, the source nable without load balancing.
Note	Unicast RPF is an end of a connection	input function and is applied only on the input interface of a router at the upstreation.

To use Unicast RPF, enable CEF switching or dCEF switching in the router. You do not need to configure the input interface for CEF switching. As long as CEF is running on the router, you can configure individual interfaces with other switching modes.

Not	e Unicast RPF will not work without CEF.
	Do not use Unicast RPF on interfaces that are internal to the network. Internal interfaces are likely to have routing asymmetry, which means that there are multiple routes to the source of a packet. You should apply Unicast RPF only where there is natural or configured symmetry.
Examples	This example shows how to enable Unicast RPF exist-only checking mode: Router(config-if)# ip verify unicast source reachable-via any Router(config-if)#
Related Command	s ip cef (refer to Cisco IOS documentation)

ip wccp group-listen

To enable the reception of IP multicast packets for the WCCP feature, use the **ip wccp group-listen** command mode. Use the **no** form of this command to disable the reception of IP multicast packets for the WCCP feature.

ip wccp {web-cache | {service-number | service-name}} group-listen

no ip wccp {**web-cache** | {*service-number* | *service-name*}} **group-listen**

Syntax Description	web-cache	Directs the router to send packets to the web cache service.
	service-number	WCCP service number; valid values are from 0 to 99.
	service-name	WCCP service name; the valid value is web-cache .
Defaults	Disabled	
Command Modes	Interface configurati	on
Command History	Release	Modification
-	12.1(13)E	This command was introduced on the MSFC.
Usage Guidelines		
Note	To ensure correct op group-listen comma	eration, you must enter the ip pim <i>mode</i> command in addition to the ip wccp nd.
	representing a cache	may be either one of the provided standard keyword definitions or a number engine dynamically defined definition. Once the service is enabled, the switch can participate in the establishment of a service group.
	On Catalyst 6500 set the following config	ries switches that are to be members of a service group when IP multicast is used, uration is required:
	• You must config	ure the IP multicast address for use by the WCCP service group.
		ure the ip wccp { web-cache <i>service-number</i> } group-listen command on the re to receive the IP multicast address.

 Examples
 This example shows how to enable the multicast packets for a web cache with a multicast address of 224.1.1.100:

 router# configure terminal
 router(config)# ip wccp web-cache group-address 244.1.1.100

 router(config)# interface ethernet 0
 router(config-if)# ip wccp web-cache group listen

Related Commands ip wccp ip wccp redirect

Catalyst 6500 Series Switch MSFC Command Reference—Release 12.1(13)E

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** command. To disable WCCP redirection, use the **no** form of this command.

ip wccp *service* **redirect** {**out** | **in**}

no ip wccp service **redirect** {**out** | **in**}

Syntax Description	service	Specifies the service group; valid values are web-cache or the identification number (from 0 to 99) of the service.
	out	Specifies packet redirection on an outbound interface.
	in	Specifies packet redirection on an inbound interface.
Defaults	WCCP redire	ect is disabled.
Command Modes	Interface con	ifiguration
Command History	Release	Modification
	12.1(13)E	This command was introduced on the MSFC.
Jsage Guidelines	receiving inb that interface	<i>service</i> redirect in command allows you to configure WCCP redirection on an interface yound network traffic. When the command is applied to an interface, all packets arriving a e will be compared against the criteria that is defined by the specified WCCP service. If the the the criteria, they will be redirected.
	The ip wccp outbound int	<i>service</i> redirect out command allows you to configure the WCCP redirection check at a cerface.
<u> </u>		ot to confuse the ip wccp service redirect { out in } interface configuration command with redirect exclude in interface configuration command.
Note		nd has the potential to affect the ip wccp redirect exclude in command. (These ave opposite functions.) If you have ip wccp redirect exclude in set on an interface and

Examples This example shows how to configure a session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Cache Engine:

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect ?
    in Redirect to a Cache Engine appropriate inbound packets
    out Redirect to a Cache Engine appropriate outbound packets
Router(config-if)# ip wccp 99 redirect out
```

This example shows how to configure a session in which HTTP traffic arriving on Ethernet interface 0/1 will be redirected to a Cisco Cache Engine:

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

Related Commands ip wccp redirect exclude in (refer to Cisco IOS documentation)

ipx network

To enable IPX routing on a particular interface and to optionally select the type of encapsulation (framing), use the **ipx network** command in interface configuration mode. To disable IPX routing, use the **no** form of this command.

ipx network network [encapsulation encapsulation-type [secondary]]

no ipx network *network* [**encapsulation** *encapsulation-type*]

Syntax Description network Network number. encapsulation (Optional) Type of encapsulation (framing). For a list of possible encapsulation types, see Table 2-1. secondary (Optional) Indicates an additional (secondary) network configured af the first (primary) network. Defaults The defaults are as follows: • IPX routing is disabled. • Encapsulation types: • For Ethernet: novell-ether • For Token Ring: sap • For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type fromovell-ether to sap. Command Modes Interface configuration
encapsulation-type encapsulation types, see Table 2-1. secondary (Optional) Indicates an additional (secondary) network configured af the first (primary) network. Defaults The defaults are as follows: • IPX routing is disabled. • Encapsulation types: • For Ethernet: novell-ether • For Token Ring: sap • For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes Interface configuration
secondary (Optional) Indicates an additional (secondary) network configured af the first (primary) network. Defaults The defaults are as follows: • IPX routing is disabled. • Encapsulation types: • For Ethernet: novell-ether • For Token Ring: sap • For FDDI: snap • For Serial: hdle If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes Interface configuration
Defaults The defaults are as follows: • IPX routing is disabled. • Encapsulation types: • For Ethernet: novell-ether • For Token Ring: sap • For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes
 IPX routing is disabled. Encapsulation types: For Ethernet: novell-ether For Token Ring: sap For FDDI: snap For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap.
 IPX routing is disabled. Encapsulation types: For Ethernet: novell-ether For Token Ring: sap For FDDI: snap For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes Interface configuration
 Encapsulation types: For Ethernet: novell-ether For Token Ring: sap For FDDI: snap For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap.
 For Ethernet: novell-ether For Token Ring: sap For FDDI: snap For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap.
 For Token Ring: sap For FDDI: snap For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes Interface configuration
 For FDDI: snap For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes Interface configuration
 For Serial: hdlc If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes Interface configuration
If you use NetWare Version 4.0 and Ethernet, you must change the default encapsulation type from novell-ether to sap. Command Modes Interface configuration
Command Modes Interface configuration
Command History Release Modification
This command was introduced on the MSFC.
Usage Guidelines The <i>network</i> is an eight-digit hexadecimal number that uniquely identifies a network cable segm can be a number in the range 1 to FFFFFFD. You do not need to specify leading zeros in the <i>network</i> number. For example, for the network number 000000AA you can enter AA.
The alt keyword is used to specify an alternate configuration and is used in the following:
[no] ipx network network [encapsulation encapsulation-type [secondary]] [alt [no] ipx net network [encapsulation encapsulation-type [secondary]]]
Table 2-1 describes the types of encapsulation available for specific interfaces.

Encapsulation Type	Description
arpa	For Ethernet interfaces only—Use Novell's Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
hdlc	For Serial interfaces only—Use HDLC encapsulation.
novell-ether	For Ethernet interfaces only—Use Novell's "Ethernet_802.3" encapsulation. This encapsulation consists of a standard 802.3 Media Access Control (MAC) header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.
novell-fddi	For FDDI interfaces only—Use Novell's "FDDI_RAW" encapsulation. This encapsulation consists of a standard FDDI MAC header followed directly by the IPX header with a checksum of 0xFFFF.
sap	• For Ethernet interfaces—Use Novell's Ethernet_802.2 encapsulation.This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 LLC header. This is the default encapsulation used by NetWare Version 3.12 and 4.0.
	• For Token Ring interfaces—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header.
	• For FDDI interfaces—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.
snap	• For Ethernet interfaces—Use Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 SNAP LLC header.
	• For Token Ring and FDDI interfaces—This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.

Table 2-1 Encapsulation Types

The **ipx network** command allows you to configure a single logical network on a physical network or more than one logical network on the same physical network (network cable segment). Each network on a given interface must have a different encapsulation type.



You cannot configure more than 200 IPX interfaces on a router using the **ipx network** command.

The first network you configure on an interface is considered to be the primary network. Any additional networks are considered to be secondary networks; these must include the **secondary** keyword.



In future Cisco IOS software releases, primary and secondary networks may not be supported.

NLSP does not support secondary networks. You must use subinterfaces in order to use multiple encapsulations with NLSP.

<u>Note</u>

te When enabling NLSP and configuring multiple encapsulations on the same physical LAN interface, you must use subinterfaces. You cannot use secondary networks.

You can configure an IPX network on any supported interface as long as all the networks on the same physical interface use a distinct encapsulation type. For example, you can configure up to four IPX networks on a single Ethernet cable because Ethernet supports four encapsulation types.

The interface processes only packets with the correct encapsulation and the correct network number. IPX networks using other encapsulations can be present on the physical network. The only effect on the router is that it uses some processing time to examine packets to determine whether they have the correct encapsulation.

All logical networks on an interface share the same set of configuration parameters. For example, if you change the IPX RIP update time on an interface, you change it for all networks on that interface.

When you define multiple logical networks on the same physical network, IPX treats each encapsulation as if it were a separate physical network. This means, for example, that IPX sends RIP updates and SAP updates for each logical network.

The **ipx network** command is useful when migrating from one type of encapsulation to another. If you are using it for this purpose, you should define the new encapsulation on the primary network.

To delete all networks on an interface, use the following command:

no ipx network

Deleting the primary network with the following command also deletes all networks on that interface. The argument *number* is the number of the primary network.

no ipx network number

To delete a secondary network on an interface, use one of the following commands. The argument *number* is the number of a secondary network.

no ipx network number

no ipx network number encapsulation encapsulation-type

Novell's FDDI_RAW encapsulation is common in bridged or switched environments that connect Ethernet-based Novell end hosts via a FDDI backbone. Packets with FDDI_RAW encapsulation are classified as Novell packets, and are not automatically bridged when you enable both bridging and IPX routing. Additionally, you cannot configure FDDI_RAW encapsulation on an interface configured for IPX autonomous or SSE switching. Similarly, you cannot enable IPX autonomous or SSE switching on an interface configured with FDDI_RAW encapsulation.

With FDDI_RAW encapsulation, platforms that do not use CBUS architecture support fast switching. Platforms using CBUS architecture support only process switching of **novell-fddi** packets received on an FDDI interface.

Examples

The following example uses subinterfaces to create four logical networks on Ethernet interface 0. Each subinterface has a different encapsulation. Any interface configuration parameters that you specify on an individual subinterface are applied to that subinterface only.

```
ipx routing
interface ethernet 0
  ipx network 1 encapsulation novell-ether
interface ethernet 0.1
  ipx network 2 encapsulation snap
interface ethernet 0.2
  ipx network 3 encapsulation arpa
interface ethernet 0
  ipx network 4 encapsulation sap
```

The following example uses primary and secondary networks to create the same four logical networks as shown previously in this section. Any interface configuration parameters that you specify on this interface are applied to all the logical networks. For example, if you set the routing update timer to 120 seconds, this value is used on all four networks.

ipx routing ipx network 1 encapsulation novell-ether ipx network 2 encapsulation snap secondary ipx network 3 encapsulation arpa secondary ipx network 4 encapsulation sap secondary

The following example enables IPX routing on FDDI interfaces 0.2 and 0.3. On FDDI interface 0.2, the encapsulation type is SNAP. On FDDI interface 0.3, the encapsulation type is Novell's FDDI_RAW.

ipx routing

interface fddi 0.2 enc sde 2
ipx network f02 encapsulation snap
interface fddi 0.3 enc sde 3
ipx network f03 encapsulation novell-fddi

Related Commands	Command

Command	Description
ipx routing	Enables IPX routing.

maximum-paths

To control the maximum number of parallel routes that an IP routing protocol can support, use the **maximum-paths** command. Use the **no** form of this command to restore the default values.

maximum-paths maximum

no maximum-paths

Syntax Description	maximum	Maximum number of parallel routes that an IP routing protocol installs in a routing table; valid values are from 1 to 8.
Defaults	The defaults	are as follows:
	• BGP is o	ne path.
	• All other	Prouting protocols is four paths.
Command Modes	Routing proto	ocol configuration
Command History	Release	Modification
	12.0(7)XE	Support for this command was introduced on the MSFC.
	12.1(1)E	Support for this command on the MSFC was extended to the E train.
	12.1(8a)E	This command was modified to change the maximum number of parallel routes from six to eight paths.
Examples	-	e shows how to allow a maximum of two paths to a destination: ig) # maximum-paths 2 ig)

mls aclmerge algorithm

To select the type of ACL merge method to use, use the mls aclmerge algorithm command.

mls aclmerge algorithm {bdd | odm}

Syntax Description	bdd	Specifies the BDD-based ACL merge function.
	odm	Specifies the ODM-based ACL merge function.
Defaults	bdd	
Command Modes	Global configura	tion
Command History	Release	Modification
	12.1(8a)EX2	Support for this command was introduced on the MSFC.
	12.1(12c)E1	Support for this command was extended to the E train. This command was change to support the ODM-based ACL merge function on both security ACLs and ACLs used for QoS filtering.
Usage Guidelines	Ines The BDD-based ACL merge function uses a method of representing Boolean function into a single merged list of TCAM entries that can be programmed into the TCAM. The ODM-based ACL merge function uses an order-dependent merge algorithm to be programmed into the TCAM.	
Note		ease12.2(14)SX, the bdd option is supported on systems configured with a Supervisor pervisor Engine 2. The bdd option is not supported on systems configured with a te 3.
Note	only security AC	r than Cisco IOS Release 12.1(12c)E1, the ODM-based ACL merge function supports Ls and does not apply to ACLs used for QoS filtering. In Cisco IOS Release later releases, the ODM-based ACL merge function supports both security ACLs and oS filtering.
		algorithm method, the change is not retroactive. For example, ACLs that have had the e not affected. The merge change applies to future merges only.

Use the show fm summary command to see the status of the current merge method.

 Examples
 This example shows how to select the BDD-based ACL merge function to process ACLs:

 Router(config)# mls aclmerge algorithm bdd

 The algorithm chosen will take effect for new ACLs which are being applied, not for already applied ACLs.

 Router(config)

 This example shows how to select the ODM-based ACL merge function to process ACLs:

 Router(config)# mls aclmerge algorithm odm

 The algorithm chosen will take effect for new ACLs which are being applied, not for already applied ACLs.

 Router(config)# mls aclmerge algorithm odm

 The algorithm chosen will take effect for new ACLs which are being applied, not for already applied ACLs.

 Router(config)#

Related Commands show fm summary

mls ip

	To enable MLS IP for the internal router on the interface, use the mls ip command. Use the no form of this command to disable MLS IP on the interface.		
	mls ip		
	no mls ip		
Syntax Description	This command has	no arguments or keywords.	
Defaults	Multicast is disabled		
Command Modes	Interface configuration		
Command History	Release	Modification	
	12.0(7)XE	Support for this command was introduced on the MSFC.	
	12.1(12c)E	This command was changed to support the Supervisor Engine 2.	
Examples	This example shows how to enable MLS IP shortcuts:		
	Router(config-if) Router(config-if)	-	
Related Commands	Reference)	e configuration mode) (refer to the Catalyst 6500 Series Switch Cisco IOS Command east (refer to the Catalyst 6500 Series Switch Cisco IOS Command Reference)	

mls ip cef load-sharing full

To set CEF load balancing to include Layer 4 ports and source IP/destination IP addresses (Layer 3), use the **mls ip cef load-sharing full** command. Use the **no** form of this command to return to the default setting.

mls ip cef load-sharing full

no mls ip cef load-sharing full

- Syntax Description This command has no arguments or keywords.
- Defaults Load balancing is based on the source IP/destination IP addresses only.
- Command Modes Global configuration

Command History	Release	Modification
	12.1(11b)E	Support for this command was introduced on the MSFC.

Usage GuidelinesThe mls ip cef load-sharing full command is supported on systems configured with the Supervisor
Engine 2 only.For additional guidelines, refer to the Catalyst 6500 Series Switch Cisco IOS Software Configuration
Guide.

 Examples
 This example shows how to set load balancing to include Layer 3 and Layer 4 ports:

 Router(config)# mls ip cef load-sharing full

 Router(config)#

 This example shows how to return to the default setting:

 Router(config)# no mls ip cef load-sharing full

 Router(config)# no mls ip cef load-sharing full

 Router(config)#

Related Commands show running-config (refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference*)

mls ip cef rate-limit

To rate limit CEF-punted data packets, use the **mls ip cef rate-limit** command. Use the **no** form of this command to disable this feature.

mls ip cef rate-limit pps

no mls ip cef rate-limit

Syntax Description	<i>pps</i> Number of data packets; valid values are from 0 to 1000000.			
Defaults	No rate limit is configured. Global configuration			
Command Modes				
Command History	Release	Modification		
	12.1(5c)EX	Support for this command was introduced on the MSFC.		
	12.1(8a)E	Support for this command was extended to the E train.		
	cannot be forw can overload th protocols. The	-of-service attacks target the route processing engines of routers. Certain packets that varded by the PFC2 are directed to the MSFC2 for processing. Denial-of-service attack he route processing engine and cause routing instability when running dynamic routing e mls ip cef rate-limit command can be used to limit the amount of traffic sent to the vent denial-of-service attacks against the route processing engine.		
	This command rate limits all CEF-punted data packets including the following:			
	Data packets going to the local interface IP address			
	Data packets requiring ARP			
	Setting the rate to a low value could impact handling of packets destined to the IP addresses of the local interfaces and packets requiring ARP.			
	You should use rates.	e this command to limit these packets to a normal rate and to avoid abnormal incoming		
	For additional	guidelines, refer to the Catalyst 6500 Series Switch Cisco IOS Software Configuration		

Guide.

Examples This example shows how to enable and set the rate-limiting feature: Router(config) # mls ip cef rate-limit 50000 Router(config) #

Related Commands set mls rate (refer to the *Catalyst 6500 Series Switch Command Reference*)

mls ip delete-threshold

Use the mls ip delete-threshold command to delete configured ACL thresholds.

mls ip delete-threshold acl-num

Syntax Description	acl-num Reflective ACL number; valid values are from 1 to 10000. This command has no default settings.			
Defaults				
Command Modes	Global configu	ration		
Command History	Release	Modification		
	12.1(12c)E1	This command was introduced on the MSFC.		
Usage Guidelines	The mls ip delete-threshold command is active only when you enable the mls ip reflexive ndr-entr tcam command.			
Examples	This example s	hows how to delete an ACL threshold:		
	Router(config) Router(config))# mls ip delete-threshold 223)#		
Related Commands	mls ip install-t mls ip reflexive	hreshold e ndr-entry tcam (refer to the Catalyst 6500 Series IOS Command Reference)		

mls ip inspect

Use the **mls ip inspect** command to permit traffic through any ACLs that would deny the traffic through other interfaces. Use the **no** form of this command to return to the default setting.

mls ip inspect *acl-name*

no mls ip inspect acl-name

Syntax Description	acl-name ACL name.				
Defaults	Permit traffic	is disabled.			
Command Modes	Global config	uration			
Command History	Release	Modification			
,	12.1E	This command was introduced on the MSFC.			
Usage Guidelines	On a Catalyst 6500 series switch, when interfaces are configured to deny traffic, the CBAC permits traffic to flow bidirectionally only through the interface that is configured with the ip inspect comman				
Examples	This example shows how to permit the traffic through a specific ACL (named deny_ftp_c): Router(config) # mls ip inspect deny_ftp_c Router(config) #				
Related Commands	ip inspect (ref	fer to Cisco IOS documentation)			

mls ip install-threshold

Use the **mls ip install-threshold** command to install the configured ACL thresholds.

mls ip install-threshold acl-num

Syntax Description	acl-num	Reflective ACL number; valid values are from 1 to 10000.	
Defaults	This command h	nas no default settings.	
Command Modes	Global configura	ation	
Command History	Release	Modification	
-	12.1(12c)E1	This command was introduced on the MSFC.	
Usage Guidelines	The mls ip install-threshold command is active only when you enable the mls ip reflexive ndr-ent tcam command.		
Examples	This example sh	ows how to install an ACL threshold:	
	Router(config) Router(config)	# mls ip install-threshold 123 #	
Related Commands	<mark>mls ip delete-th</mark> mls ip reflexive <i>Reference</i>)	reshold ndr-entry tcam (refer to the Catalyst 6500 Series Switch Cisco IOS Command	

mls ip multicast consistency-check

To enable and configure the hardware shortcut consistency checker, use the **mls ip multicast consistency-check** command. Use the **no** form of this command to disable the consistency checkers.

mls ip multicast consistency-check [{**settle-time** *seconds*} | {**type scan-mroute** [**count** *count-number*] | {**settle-time** *seconds*}]

no mls ip multicast consistency-check

Syntax Description	settle-time	(Optional) Specifies the settle time for entry/oif for the consistency
	seconds	checker; valid values are from 2 to 3600 seconds.
	type	(Optional) Specifies the type of consistency check as a scan check of the
	scan-mroute	mroute table.
	count	(Optional) Specifies the maximum number of prefixes to check per
	count-number	scan; valid values are from 2 to 500.
	period seconds	Specifies the period between scans; valid values are from 2 to 3600 seconds.
Defaults	 count count- period second	as follows: check is enabled. number is 20. ads is 2 seconds. econds is 60 seconds.
Command Modes	Global configuration	
Command History	Release	Modification
	12.1(12c)E4	Support for this command was introduced on the MSFC.
Usage Guidelines	The consistency of consistent with the automatically consistent with the automatically consistence of the second s	g interface of a multicast {*,G} or {source, group} flow. checker scans the mroute-table and assures that the multicast-hardware entries are ne mroute-table. Whenever an inconsistency is detected, the inconsistency is rected. consistency error, use the show mls ip multicast consistency-check command.
	is display the in	sonoistene, erer, ase the brow mis ip muticust consistency check command.

Examples	This example shows how to enable the hardware shortcut consistency checker:			
	Router (config)# mls ip multicast consistency-check Router (config)#			
	This example shows how to enable the hardware shortcut consistency checker and configure the scan check of the mroute table:			
	Router (config)# mls ip multicast consistency-check type scan-mroute count 20 period 35 Router (config)#			
	This example shows how to enable the hardware shortcut consistency checker and specify the period between scans:			
	Router (config)# mls ip multicast consistency-check type scan-mroute period 35 Router (config)#			

Related Commandsshow mls ip multicast consistency-check (refer to the Catalyst 6500 Series Switch Cisco IOS Command
Reference

2-41

mls ip multicast stub

To enable support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **mls ip multicast stub** command. Use the **no** form of this command to disable this feature.

mls ip multicast stub

no mls ip stub

Syntax Description	This command has no arguments or keywords.		
Defaults	Multicast is disabled		
Command Modes	Interface configuration		
Command History	Release	Modification	
	12.2(14)SX	Support for this command was introduced on the MSFC.	
Usage Guidelines	command on th	ble the ACL-based method of filtering RPF failures by entering the mls ip multicast stub he redundant router, the following ACLs automatically download to the PFC and are interface that you specify:	
	• access-list 100 permit ip A.B.C.0 0.0.0.255 any		
	• access-list 100 permit ip A.B.D.0 0.0.0.255 any		
	 access-list 	• access-list 100 permit ip any 224.0.0.0 0.0.255	
	 access-list 100 permit ip any 224.0.1.0 0.0.0.255 access-list 100 deny ip any 224.0.0.0 15.255.255.255 The ACLs filter RPF failures and drop them in hardware so that they are not forwarded to the Use the ACL-based method of filtering RPF failures only in sparse-mode stub networks when o downstream routers. For dense mode groups, RPF failure packets have to be seen on the the PIM assert mechanism to function properly. Use CEF-or NetFlow-based rate limiting to RPF failures in dense-mode networks and sparse-mode transit networks. 		
Examples	This example s networks:	shows how to enable support for non-RPF traffic drops for PIM sparse-mode stub	
	Router(config Router(config	<pre>g-if)# mls ip multicast stub g-if)#</pre>	
Related Commands	show mls ip m	nulticast (refer to the Catalyst 6500 Series Switch Cisco IOS Command Reference)	

mtu

To adjust the maximum packet size or MTU size, use the **mtu** command. Use the **no** form of this command to return to the default value.

mtu bytes

no mtu

Syntax Description	bytes	Byte size; valid values are from 64 to 9216 for SVI ports and from 1500
		to 9216 for all other ports.

Defaults

Table 2-2 lists the default MTU values if jumbo frame support is disabled.

Table 2-2 Default MTU Values

Media Type	Default MTU (bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

If you enable jumbo frame support, the default is 64 for SVI ports and 9216 for all other ports. Jumbo frame support is disabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	12.1(8a)EX	Support for this command was introduced on the MSFC.
	12.1(11b)EX	This command was changed to support jumbo frames.
	12.1(13)E	Support for this command was extended to the E train.

Usage Guidelines	For switch ports, only one larger-than-default MTU value is allowed globally. For Layer 3 ports, including router ports and VLANs, you can configure nondefault MTU values on a per-interface basis.			
	For a complete list of modules that do not support jumbo frames, refer to the <i>Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide</i> .			
	Changing the MTU value with the mtu command can affect values for the protocol-specific versions of the command (for example, the ip mtu command). If the values specified with the ip mtu command is the same as the value specified with the mtu command, and you change the value for the mtu command, the ip mtu value automatically matches the new mtu command value. However, changing the values for the ip mtu command has no effect on the value for the mtu command.			
Examples	This example shows how to specify an MTU of 1800 bytes:			
	Router(config)# interface fastethernet 5/1 Router(config-if)# mtu 1800			
Related Commands	ip mtu (refer to the Cisco IOS Release 12.1 Command Reference)			

redundancy

To enable redundancy and enter the redundancy configuration mode, use the redundancy command.

redundancy

- **Syntax Description** This command has no arguments or keywords.
- **Defaults** This command has no default settings.
- Command Modes Global configuration

٠

Command History	Release	Modification
	12.1E	This command was introduced on the MSFC.

Usage Guidelines Once you enter redundancy configuration mode, these options are available:

- exit—Exits from redundancy configuration mode.
- **high-availability**—Enters high-availability redundancy configuration mode. See the **high-availability** command for additional information.
- no-Negates a command or set its defaults.

 Examples
 This example shows how to enable redundancy and enter the redundancy configuration submode:

 Router(config) # redundancy
 Router(config-r) #

Related Commands high-availability show redundancy

set traffic-index

To create a BGP traffic classification number for accounting, use the set traffic-index command.

set traffic-index num

Syntax Description	<i>num</i> Nu	mber of the bucket; valid values are from 1 to 7.	
Defaults	This command h	as no default settings.	
Command Modes	Route map confi	guration	
Command History	Release	Modification	
	12.1E	This command was introduced on the MSFC.	
Usage Guidelines	Inbound and outbound traffic-shaping is based on destination traffic-index called DSTS. Destination sensitive billing provides packet and byte counters (seven sets per inbound interface), which represent counts for IP packets by destination network. It uses route maps to classify the traffic into one of seven possible indexes, which represent a traffic classification.		
Examples	This example sh	ows how to create a BGP traffic index:	
	Router(config- Router(config-	route-map)# set traffic-index 3 route-map)	

show fm features

To display information about the general feature manager, use the show fm features command.

show fm features Syntax Description This command has no keywords or arguments. Defaults This command has no default settings. **Command Modes** EXEC Modification **Command History** Release 12.1E This command was introduced on the MSFC. Examples This example shows how to display information about the general feature manager: Router> show fm features Designated MSFC:1 Non-designated MSFC:1 Redundancy Status:designated Interface:FastEthernet2/10 IP is enabled hw[EGRESS] = 1, hw[INGRESS] = 1 hw force default[EGRESS] = 0, hw force default[INGRESS] = 0 mcast = 0priority = 2reflexive = 0inbound label:1 protocol:ip feature #:1 feature id:FM IP ACCESS ACL:106 outbound label:2 protocol:ip feature #:1 feature id:FM_IP_ACCESS ACT 106 Interface:FastEthernet2/26 IP is enabled hw[EGRESS] = 1, hw[INGRESS] = 0 hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 1 mcast = 0priority = 2reflexive = 0inbound label:24 protocol:ip feature #:1 feature id:FM_IP_ACCESS ACL:113 outbound label:3 protocol:ip feature #:1 feature

```
id:FM IP WCCP
          Service ID:0
          Service Type:0
Interface:Vlan55 IP is enabled
  hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:4
        protocol:ip
          feature #:1
          feature id:FM IP ACCESS
         ACL:111
Interface:Vlan101 IP is enabled
 hw[EGRESS] = 1, hw[INGRESS] = 1
  hw_force_default[EGRESS] = 0, hw_force_default[INGRESS] = 0
  mcast = 0
  priority = 2
  reflexive = 0
  inbound label:5
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
         ACL:101
  outbound label:6
        protocol:ip
          feature #:1
          feature id:FM_IP_ACCESS
          ACL:101
Router>
```

This example shows how to display lines of general feature manager information beginning with the line that begins with Redundancy:

Router> **show fm features** | **begin Redundancy** Redundancy Status: designated Router>

show fm inband-counters

To display the number of inband packets sent by the MSFC for SLB and WCCP, use the **show fm inband-counters** command.

show fm inband-counters

Syntax Description	This command has no keywords or arguments.		
Defaults	This command has	no default settings.	
Command Modes	EXEC		
Command History	Release	Modification	
	12.1(8a)E2	Support for this command was introduced on the MSFC.	
		the number of WCCP inband packets that were sent. ared, the display includes the number of packets that were sent for CBAC.	
	If CBAC is configu	ared, the display includes the number of packets that were sent for CBAC.	
Examples	This example show Router# show fm :	vs how to display the number of SLB and WCCP inband packets that were sent:	
	Inband Pacl		
	Slot WCCP	SLB	
	1 0	0	
	2 0	0	
	3 0	0	
	4 0	0	
	5 0	0	
	6 0	0	
	7 0	0	
	8 0	0	
	9 0	0	

Router#

10

11

12

13

0

0

0

0

0

0

0 0

show fm insp

To display the list and status of the ACLs and ports on which CBAC is configured, use the **show fm insp** command.

show fm insp [detail]

Syntax Description	detail	(Optional) Displays all of the flow information.		
Defaults	This command h	as no default settings.		
Command Modes	EXEC			
Command History	Release	Modification		
	12.1(6)E	Support for this command was introduced on the MSFC.		
Usage Guidelines	If you can configure a VACL on the port before you configure CBAC, the status displayed is INACTIVE; otherwise, it is ACTIVE. If PFC resources are exhausted, the command displays BRIDGE followed by the number of failed currently active NetFlow requests that have been sent to the MSFC2 for processing.			
	The show fm insp command output includes this information:			
	• interface:—Interface on which the IP inspect feature is enabled.			
	 (direction)—Direction in which the IP inspect feature is enabled (IN or OUT). acl name:—Name used to identify the packets that are being inspected. 			
	 status:—(ACTIVE or INACTIVE) tells you if HW-assist is provided for this interface+direction (ACTIVE=hardware assisted or INACTIVE). 			
	The detail option interface direction	n also displays the ACEs that are part of the ACL that is used for IP inspect on the given on.		
Examples	This example sho	ows how to display the list and status of CBAC-configured ACLs and ports:		
	acl na	n insp Face:Vlan305(in) status :ACTIVE ame:deny arfaces:		

```
interfaces:
    Vlan305(out):status ACTIVE
```

show fm interface

To display the detailed information about the feature manager on a per-interface basis, use the **show fm interface** command.

show fm interface {{interface interface-number} | {null interface-number} | {port-channel
 number} | {vlan vlan-id}}

Syntax Description	interface	Interface type; possible valid values are pos , atm , and ge-wan .		
- ,	interface-number	Module and port number; see the "Usage Guidelines" section for valid values.		
	null interface-number	Specifies the null interface; the valid value is 0 .		
	vlan vlan-id	Specifies the VLAN; see the "Usage Guidelines" section for a list of valid values.		
Defaults	This command has	no default settings.		
Command Modes	EXEC			
Command History	Release	Modification		
	12.1(1)E	Support for this command was introduced on the MSFC.		
Usage Guidelines	The <i>interface-number</i> argument designates the module and port number. Valid values for <i>interface-number</i> depend on the specified interface type and the chassis and module used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module installed in a Catalyst 6513 chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.			
	your system is conf	onfigured with a Supervisor Engine 1, valid values for <i>vlan-id</i> are from 1 to 1005. If igured with a Supervisor Engine 2, valid values for <i>vlan-id</i> are from 1 to 4094. ANs are not supported on systems configured with a Supervisor Engine 1.		
Examples	This example shows how to display the detailed information about the feature manager on a specified interface:			
	<pre>Interface:FastEth hw[EGRESS] = 1,</pre>			

```
feature #:1
          feature id:FM_IP_ACCESS
          ACL:113
                vmr IP value #1:0, 0, 0, 0, 0, 0, 0, 6 - 1
                vmr IP mask #1:0, 0, FFFF, FFFF, 0, 0, 0, FF
                vmr IP value #2:642D4122, 0, 0, 0, 1, 0, 0, 6 - 1
                vmr IP mask #2:FFFFFFF, 0, 0, 0, 1, 0, 0, FF
                vmr IP value #3:0, 64020302, 0, 0, 6, 0, 0, 6 - 1
                vmr IP mask #3:0, FFFFFFF, 0, 0, 6, 0, 0, FF
                vmr IP value #4:0, 64020302, 0, 0, A, 0, 0, 6 - 1
                vmr IP mask #4:0, FFFFFFF, 0, 0, A, 0, 0, FF
                vmr IP value #5:0, 64020302, 0, 0, 12, 0, 0, 6 - 1
                vmr IP mask #5:0, FFFFFFF, 0, 0, 12, 0, 0, FF
                vmr IP value #6:0, 0, 0, 0, 0, 0, 0, 0 - 2
                vmr IP mask #6:0, 0, 0, 0, 0, 0, 0, 0
  outbound label:3
       protocol:ip
          feature #:1
          feature id:FM IP WCCP
          Service ID:0
          Service Type:0
Router>
```

show fm reflexive

To display information about the dynamic feature manager reflexive entry, use the **show fm reflexive** command.

show fm reflexive

Syntax Description	This command has r	no keywords or arguments.
Defaults	This command has n	no default settings.
Command Modes	EXEC	
Command History	Release 12.1E	Modification Support for this command was introduced on the MSFC.
Examples	Router# show fm re Reflexive h	
	Router#	

show fm summary

To display a summary of feature manager information, use the show fm summary command.

	show fm sum	mary	
Syntax Description	This command has	s no keywords or arguments.	
Defaults	This command has	s no default settings.	
Command Modes	EXEC		
Command History	Release	Modification	
	12.1E	Support for this command was introduced on the MSFC.	
Examples	Router# show fm	ws how to display a summary of feature manager information: summary CL merge algorithm:BDD	

show fm vlan

To display information about the per-VLAN feature manager, use the show fm vlan command.

show fm vlan vlan-id

Syntax Description	<i>vlan-id</i> VLAN number; see the "Usage Guidelines" section for valid values.		
Defaults	This command has i	no default settings.	
Command Modes	EXEC		
Command History	Release	Modification	
	12.1(11b)EX	Support for this command was introduced on the Catalyst 6500 series switches.	
	12.1(13)E	Support for this command on the Catalyst 6500 series switches was extended to the E train.	
Usage Guidelines	your system is confi	nfigured with a Supervisor Engine 1, valid values for <i>vlan-id</i> are from 1 to 1005. If igured with a Supervisor Engine 2, valid values for <i>vlan-id</i> are from 1 to 4094. ANs are not supported on systems configured with a Supervisor Engine 1.	
Examples	This example shows	s how to display information about the per-VLAN feature manager:	
	<pre>mcast = 0 priority = 2 reflexive = 0 vacc_map : map1 inbound label: 5 merge_err: 0 protocol: ip feature #: 1 feature id: FM_VAG map_name: map1 seq #: 10 (only for IP_PROT) vmr IP value # 1: vmr IP mask # 1: 0 vmr IP value # 2: vmr IP mask # 2: 0 vmr IP value # 3: vmr IP mask # 3: 0 seq #: 65536</pre>	w[INGRESS] = 1 EGRESS] = 0, hw_force_default[INGRESS] = 0	

```
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
outbound label: 6
merge err: 0
protocol: ip
feature #: 1
feature id: FM_VACL
map_name: map1
seq #: 10
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L4OP TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 6 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 FF
vmr IP value # 2: 0.0.0.0 0.0.0.0 0 0 0 0 11 permit
vmr IP mask # 2: 0.0.0.0 0.0.0.0 0 0 0 0 FF
vmr IP value # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 deny
vmr IP mask # 3: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
seq #: 65536
(only for IP_PROT) DestAddr SrcAddr Dpt Spt L40P TOS Est prot Rslt
vmr IP value # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0 permit
vmr IP mask # 1: 0.0.0.0 0.0.0.0 0 0 0 0 0 0
```

show ip auth-proxy watch-list

To display the authentication proxy watch list information, use the **show ip auth-proxy watch-list** command.

show ip auth-proxy watch-list

- Syntax Description This command has no arguments or keywords.
- **Defaults** This command has no default settings.

Command Modes EXEC

 Release
 Modification

 12.1(13)E
 This command was introduced on the MSFC.

Examples Router# show ip auth-proxy watch-list Authentication Proxy Watch-list is enabled Watch-list expiry timeout is 2 minutes Total number of watch-list entries: 3 Source IP Violation-count Type 12.0.0.2 MAX_RETRY MAX_LIMIT 12.0.0.3 TCP_NO_DATA MAX_LIMIT 1.2.3.4 CFGED N/A Total number of watch-listed users: 3 Router#

Related Commands clear ip auth-proxy watch-list ip auth-proxy max-login-attempts ip auth-proxy watch-list

show ip wccp web-cache detail

To display statistics for only the first packet of a Layer 2 redirected flow, use the **show ip wccp web-cache detail** command.

show ip wccp web-cache detail

Syntax Description	This command has no keywords or arguments.			
Defaults	This command has no default settings.			
Command Modes	EXEC			
Command History	Release	Modification	l	
	12.1(2)E	Support for t	this command was introduced on the MSFC.	
Usage Guidelines	Use the show ip wccp web-cache detail command to provide an indication of how many flows, rather than packets, are using Layer 2 redirection. For additional information regarding IP WCCP commands, refer to the section "Configuring Web Cache Services Using WCCP" in the <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> .			
Examples	This example displays the connected cache engine using Layer 2 redirection:			
	Router # show ip wccp web-cache detail WCCP Cache-Engine information: IP Address: 10.11.1.1 Protocol Version: 2.0 State: Usable Redirection: L2 Initial Hash Info: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF			

Table 2-3 describes the fields shown in the example.

Field	Description		
WCCP Cache-Engine information	Header for the area that contains the fields for the IP address and the version of WCCP associated with the router connected to the cache engine in the service group.		
IP Address	IP address of the router connected to the cache engine in the service group.		
Protocol Version	Version of WCCP that is used by the router in the service group.		
WCCP Cache-Engine information	Fields for information on the cache engines.		
IP Address	IP address of the cache engine in the service group.		
Protocol Version	Version of WCCP that is used by the cache engine in the servi group.		
State	Status of whether the cache engine is operating properly and can be contacted by a router and other cache engines in the service group.		
Initial Hash Info	Initial state of the hash bucket assignment.		
Assigned Hash Info	Current state of the hash bucket assignment.		
Hash Allotment	Percentage of buckets assigned to the current cache engine. Both a value and a percent figure are displayed.		
Packets Redirected	Number of packets that have been redirected to the cache engine.		
Connect Time Amount of time it took for the cache engine to conrouter.			

Table 2-3 show ip wccp web-cache detail Command Output Fields

Related Commands

clear ip wccp (refer to Cisco IOS documentation)ip wccp (refer to Cisco IOS documentation)show ip interface (refer to Cisco IOS documentation)

show I3-mgr

To display Layer 3 manager information, use the **show l3-mgr** command.

show 13-mgr status

show l3-mgr {interface {{interface interface-number} | {null interface-number} |
{port-channel number} | {vlan vlan-id} | status}}

Syntax Description	status	Displays the global argument information.			
	interface	Displays the interface detailed Layer 3 manager information.			
	interface	Interface type; possible valid values are pos , atm , and ge-wan .			
	interface-number	Module and port number; see the "Usage Guidelines" section for valid values.			
	null interface-number	Specifies the null interface; the valid value is 0 .			
	vlan vlan-id	Specifies the VLAN; see the "Usage Guidelines" section for valid values.			
	status	Specifies the Layer 3 manager status information.			
Command Modes	EXEC				
Command History	Release	Modification			
	12.1E	This command was introduced on the MSFC.			
Usage Guidelines	only.	eful for debugging purposes and the output is intended for TAC and engineering use			
	The <i>interface-number</i> argument designates the module and port number. Valid values for <i>interface-number</i> depend on the specified interface type and the chassis and module used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module installed in a Catalyst 6513 chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.				
	If your system is configured with a Supervisor Engine 1, valid values for <i>vlan-id</i> are from 1 to 1005. If your system is configured with a Supervisor Engine 2, valid values for <i>vlan-id</i> are from 1 to 4094. Extended-range VLANs are not supported on systems configured with a Supervisor Engine 1.				

2-59

Examples

This example shows how to display Layer 3 manager status information:

```
Router# show 13-mgr status
13_mgr_state:
                      2
13_mgr_req_q.count:
                      0
13 mgr req q.head:
                     0
l3_mgr_req_q.tail:
                     0
l3_mgr_max_queue_count: 1060
13_mgr_shrunk_count: 0
13_mgr_req_q.ip_inv_count:
                              303
13_mgr_req_q.ipx_inv_count:
                              0
13_mgr_outpak_count: 18871
l3_mgr_inpak_count: 18871
13_mgr_max_pending_pak: 4
13_mgr_pending_pak_count: 0
nde enable statue:
                     0
```

current nde addr: 0.0.0.0

```
Router#
```

This example shows how to display Layer 3 manager information for a specific interface:

Router# show 13-mgr interface ge-wan 5/40 vlan: 0 ip enabled: 1 ipx enabled: 1 bg_state: 0 0 0 0 hsrp_enabled: 0 hsrp_mac: 0000.0000.0000 state: 0 0 up: Router#

show microcode

To display the versions for all bundled MCP and LCP images for the runtime supervisor engine image, use the **show microcode** command.

show microcode

Syntax Description This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes EX

EXEC

Command History	Release	Modification
12.1E		This command was introduced on the MSFC.

Examples

This example shows how to display microcode versions:

Console> (enable) show microcode

Bundled Images	Version	Size	Built
LCP SLCP	6.2(0.92)	330918	02/16/01 01:26:27
LCP LX1000	6.2(0.92)	312782	02/16/01 01:27:59
LCP LX10100	6.2(0.92)	364846	02/16/01 01:26:47
LCP AX10100	6.2(0.92)	380296	02/16/01 01:27:10
LCP AX1000	6.2(0.92)	338672	02/16/01 01:28:19
LCP VX10100	6.2(0.92)	378532	02/16/01 01:27:35
LCP CPSLCP	6.2(0.92)	585234	02/16/01 00:59:19
LCP CPFAB	6.2(0.92)	251186	02/16/01 01:02:58
LCP CPGBIT	6.2(0.92)	579282	02/16/01 01:00:49
LCP CP10G	6.2(0.92)	477778	02/16/01 01:02:17
LCP CPMBIT2	6.2(0.92)	777922	02/16/01 01:05:20
Console> (enabl	e) show		

show msfc2 rom-monitor

To display the ROMMON region status, use the show msfc2 rom-monitor command.

show msfc2 rom-monitor

Syntax Description This command has no arguments or key	words.
---	--------

- **Defaults** This command has no default settings.
- Command Modes EXEC

 Release
 Modification

 12.1E
 This command was introduced on the MSFC.

Examples This example shows how to display ROMMON information:

Router# show msfc2 rom-monitor

Region region1: APPROVED, preferred Region region2: INVALID Currently running ROMMON from region1 region Router#

Table 3-4 describes the possible output fields for the **show msfc2 rom-monitor** command.

FieldDescriptionRegion region1 and
region2ROMMON image status and the order of preference that
region1 or region2 images should be booted from.First runROMMON image status indicating a check of the new image
that is run.InvalidROMMON image status indicating the new image has been
checked and the upgrade process has started.ApprovedROMMON image status indicating the ROMMON field
upgrade process has completed.

Current running image and the region.

Table 3-4show msfc2 rom-monitor Command Output Fields

Related Commands upgrade rom-monitor

Currently running

show redundancy

To display redundancy high-availability setting information, use the show redundancy command.

	show redu	Idancy
Syntax Description	This command l	nas no arguments or keywords.
Defaults	This command l	nas no default settings.
Command Modes	EXEC	
Command History	Release	Modification This command was introduced on the MSFC.
Examples	Router# show r Designated Rou Redundancy Sta Config Sync Ad Config Sync Ru Single Router Single Router	ows how to display information about the RF client: edundancy ter: 2 Non-designated Router: 0 tus: designated minStatus : enabled ntimeStatus: disabled Mode AdminStatus : disabled Mode RuntimeStatus: disabled Mode transition timer : 120 seconds

show scp

To display SCP information, use the **show scp** command.

show scp {accounting | counters | {process [id]} | status}

Syntax Description	acco	ounting	3	Di	splays	s SCP	accou	inting	infori	natior	ı.				
	cour	nters		Di	splays	s SCP	count	er info	ormati	ion.					
	proc	cess id		Di	splays	s infor	matio	n for a	a spec	ific p	rocess	and p	roces	s ID.	
	stat	us		Di	splays	s local	SCP	servei	statu	s info	rmatio	on.			
Defaults	This	comma	and ha	as no	defau	lt sett	ings.								
Command Modes	EXE	С													
Command History	Rele	ase			M	lodific	ation								
-	12.1	E			T	his co	mman	d was	intro	duced	on th	e MSI	FC.		
Examples	This	examp	le sho	ows h	ow to	displa	y SC	P acco	ounting	g info	rmatio	on:			
	Rout	er> sh	ow sc	p aco	count	ing									
		Total		1D	1E	2C	82	100	105	10F	119	11C	11D	11E	127
	Tot:	10F8	FFC1		2	3	1	0	1	2	2	1	6	E	110E
	11:	10FB 10F8			2 2	3 3	1 1	2 0	1 1	2 2	3 2	1 1	6 6	E E	110E 110E
		10FA	FFC1	2	2	3	1	1	1	2	3	1	6	Е	110E
	13:	0 1	0 0	0 0	0 0	0 0	0 0	0 1	0 0	0 0	0 0	0 0	0 0	0 0	0 0
											0	0			
						0									0
		1 12B	157	1FF 		Ū									°
	Tot:	12B 1	157 4	 2		Ū									°
		12B 1 1	157 4 4	 2 2		Ū									°
	11:	12B 1 1 1 1	157 4 4 4 4 4	2 2 2 2 2		Ū									Ŭ
		12B 1 1 1 1 0	157 4 4 4 4 4 0	 2 2 2		Ū									,

This example shows how to display SCP counter information:

Router> show scp counters						
received packets = 698						
transmitted packets	69894					
retransmitted packets	=	0				
loop back packets	=	0				
transmit failures = 0						
recv pkts not for me	=	0				
recv pkts to dead process	=	0				
recv pkts not enqueuable	=	0				
response has wrong opcode	=	0				
response has wrong seqnum	=	0				
response is not an ack	=	0				
response is too big	=	0				
Router>						

This example shows how to display the process name and the number of messages received and transmitted:

Rou	ter# show scp pro	cess						
PID	Process	Msgs	Msgs	NMP Tx Q	Msgs	Bufs	Rx Q	Rx Q
		Sent	Resent	in Overflow	Rcvd	Held	Size	Oflow
0	Kernel and Idle	2	0	0	0	0	0	0
1	Flash MIB Updat	0	0	0	0	0	0	0
2	SynDiags	1410	0	0	1410	0	4	0
3	SynConfig	2	0	0	3481603	0	64	0
4	Statuspoll	3481589	0	0	0	0	2	0
5 S	L_TASK	0	0	0	0	0	24	0

This example shows how to display local SCP server status information:

Router> show scp status		
Rx 69866, Tx 69864, Sap 6		
Id Channel name	<pre># msgs pending</pre>	# peak count
0 SCP async: TCAM MGR Chann	0	5
1 SCP async: 13_mgr scp cha	0	1
2 SCP async: 13_mgr scp cha	0	2
3 SCP async: Draco-NMP	0	1
Router>		

show slot0:

To display information about the slot0: file system, use the **show slot0:** command.

show slot0: [all | chips | filesys]

Syntax Description	all	(Optional) Displays all Flash information including the output from the show slot0: chips and show slot0: filesys commands.
	chips	(Optional) Displays Flash chip information.
	filesys	(Optional) Displays file system information.
Defaults	This comma	nd has no default settings.
Command Modes	EXEC	
Command History	Release	Modification
-	12.1E	This command was introduced on the MSFC.
	1 imag	rpecrcseek nlen -lengthdate/time name ge 6375DBB7 A4F144 6 10678468 Nov 09 1999 10:50:42 halley ces available (10678596 bytes used)
	This exampl	e shows how to display Flash chip information:
		ow slot0: chips htel Series 2+ Status/Register Dump *******
	Config Op Config St Card Stat Write Pro Voltage O	MEMORY REGISTERS: btion Reg (4000): 2 catus Reg (4002): 0 cus Reg (4100): 1 btect Reg (4104): 4 Chtrl Reg (410C): 0 Mode Reg (4140): 2
	Intellige	DRY REGISTERS: Bank 0 ent ID Code : 8989A0A0 .e Status Reg: 8080 Status Reg: B0B0

Block Status Regs: 0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 BOBO 24 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 BOBO COMMON MEMORY REGISTERS: Bank 1 Intelligent ID Code : 8989A0A0 Compatible Status Reg: 8080 Global Status Reg: B0B0 Block Status Regs: 0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 BOBO 8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 BOBO 16 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 BOBO COMMON MEMORY REGISTERS: Bank 2 Intelligent ID Code : 8989A0A0 Compatible Status Reg: 8080 Global Status Reg: B0B0 Block Status Regs: 0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 BOBO COMMON MEMORY REGISTERS: Bank 3 Intelligent ID Code : 8989A0A0 Compatible Status Reg: 8080 Global Status Reg: B0B0 Block Status Regs: 0 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 8 : B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 B0B0 BOBO COMMON MEMORY REGISTERS: Bank 4 Intelligent ID Code : FFFFFFF IID Not Intel -- assuming bank not populated Router> This example shows how to display file system information: Router> show slot0: filesys ----- F I L E SYSTEM STATUS -----Device Number = 0DEVICE INFO BLOCK: slot0 Magic Number = 6887635 File System Vers = 10000 (1,0)= 1000000 Length Sector Size = 20000 Programming Algorithm = 4 Erased State = FFFFFFFF File System Offset = 20000 Length = FA0000MONLIB Offset = 100Length = F568Bad Sector Map Offset = 1FFF0 Length = 10Squeeze Log Offset = FC0000 Length = 20000 Squeeze Buffer Offset = FE0000 Length = 20000Num Spare Sectors = 0 Spares: STATUS INFO: Writable NO File Open for Write

Complete Stats

No Unrecovered No Squeeze in p USAGE INFO:			
Bytes Used	= 9F365C	Bytes Available	= 5AC9A4
Bad Sectors	= 0	Spared Sectors	= 0
OK Files	= 1	Bytes = 9F35DC	
Deleted Files	= 0	Bytes = 0	
Files w/Errors	= 0	Bytes = 0	

Router>

show standby delay

To display HSRP information about delay periods, use the **show standby delay** command.

show standby delay [type number]

Syntax Description	type number	(Optional) Interface type and number for which output is displayed.
Defaults	This command has	no default settings.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.1(13)E	Support for this command was introduced on the MSFC.
Examples	This example shows	s the output from the show standby delay command:
	Interface VLAN100 1 Router#	Minimum Reload 5
Related Commands	standby delay min	imum reload

snmp-server enable traps

To enable SNMP notifications (traps or informs) available on your system, use the **snmp-server enable traps** command. To disable all available SNMP notifications, use the **no** form of this command.

snmp-server enable traps [notification-type]

no snmp-server enable traps [notification-type]

Syntax Description	notification-type	(Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled. See the "Usage Guidelines" section for valid values.				
	notification-option	<i>i</i> (Optional) Notification option. See the "Usage Guidelines" section for valid values.				
Defaults		lisabled by default. Most notification types are disabled. However, some notification ntrolled with this command.				
	If you enter this co are enabled.	mmand without a <i>notification-type</i> , all notification types controlled by this command				
	If enabled, the def	ault settings are as follows:				
	• interval secon	ads is 30				
	• fail-interval seconds is 0					
Command Modes	Global configurati					
Command History	Release	Modification				
,	12.1(11b)E	Support for this command was introduced on the Catalyst 6500 series switches.				
Usage Guidelines	For additional noti	fication types, refer to Cisco IOS documentation.				
	requests for the spe	s can be sent as traps or inform requests. This command enables both traps and inform ecified notification types. To specify whether the notifications should be sent as traps s snmp-server host [traps informs] command.				
	are sent. In order t snmp-server enab	an snmp-server enable traps command, no notifications controlled by this command o configure the router to send these SNMP notifications, you must enter at least one le traps command. If you enter the command with no keywords, all notification types enter the command with a keyword, only the notification type related to that keyword				
	is enabled. In orde	r to enable multiple types of notifications, you must issue a separate le traps command for each notification type and notification option.				

Valid values for the *notification-type* are as follows:

- **atm**—Enables ATM PVC notifications. When you enter **atm pvc**, you can specify additional *notification-option* values.
- **bgp**—Enables the BGP state change notifications
- config—Enables the configuration notifications
- dlsw—Enables the DLSw notifications
- entity—Enables the entity notifications
- frame-relay—Enables the frame-relay notifications
- hsrp—Enables the HSRP notifications
- isdn—Enables the ISDN traps. When you enter isdn, you can specify a *notification-option* value.
- **rsvp**—Enables the RSVP flow change notifications
- rtr—Enables the Response Time Reporter notifications
- snmp—Enables the SNMP notifications. When you enter snmp, you can specify additional notification-option values
- syslog—Enables error message notifications (Cisco Syslog MIB)

Valid values for the notification-option are as follows:

- atm pvc [interval seconds] [fail-interval seconds]
 - The optional **interval** *seconds* specifies the minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval in order to prevent trap storms. No traps are sent until the interval lapses.
 - The optional **fail-interval** seconds specifies the minimum period for storing the failed time stamp, in the range from 0 to 3600.
- dlsw [circuit] [tconn]
 - The optional circuit enables SNMP DLSw circuit traps.
 - The optional tconn enables SNMP DLSw peer transport connection traps
- isdn [call-information] | [layer2]
 - The optional **call-information** enables an SNMP ISDN call information notification for the ISDN MIB subsystem.
 - The optional layer2 enables SNMP ISDN Layer 2 transition traps.
- snmp [authentication] | [warmstart]
 - The optional authentication enables the authentication trap.
 - The optional **warmstart** enables the warmStart trap.

Use of the **authentication** keyword produces the same effect as not using the **authentication** keyword. Both the **snmp-server enable traps snmp** and **snmp-server enable traps snmp authentication** forms of this command will globally enable (or, if using the **no** form, disable) the following SNMP traps:

- authentication Failure
- linkUp
- linkDown
- coldstart

 Examples
 This example shows how to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

 Router(config)# snmp-server enable traps
 Router(config)# snmp-server host myhost.cisco.com public

Related Commands Refer to Cisco IOS documentation for additional **snmp-server enable traps** commands.

2-73

standby delay minimum reload

To configure the delay period before the initialization of HSRP groups, use the **standby delay minimum reload** command. Use the **no** form of this command to disable the delay period.

standby delay minimum [min-delay] reload [reload-delay]

no standby delay minimum [min-delay] reload [reload-delay]

Syntax Description	min-delay	(Optional) Minimum time, in seconds, to delay HSRP group initialization after an interface comes up; valid values are from 0 to 10000.
	reload-delay	(Optional) Time, in seconds, to delay after the router has reloaded; valid values are from 0 to 10000.
Defaults	The defaults are a	as follows:
	• <i>min-delay</i> is	1 second
	• reload-delay	is 5 seconds
Command Modes	Interface configu	ration
Command History	Release	Modification
ooninana mistory	Kelease	Mounication
	12.1(13)E	Support for this command was introduced on the MSFC.
	12.1(13)E	
Usage Guidelines	12.1(13)E The minimum dependence of	Support for this command was introduced on the MSFC.
	12.1(13)E The minimum de The delay period If the active route new active router	Support for this command was introduced on the MSFC. lay period applies to all subsequent interface events. applies only to the first interface-up event after the router has reloaded. er fails or is removed from the network, the standby router automatically becomes the
	12.1(13)EThe minimum deThe delay periodIf the active routenew active routeras the active routeHowever, even ifactive role after ito set a delay per	Support for this command was introduced on the MSFC. lay period applies to all subsequent interface events. applies only to the first interface-up event after the router has reloaded. er fails or is removed from the network, the standby router automatically becomes the . If the former active router comes back online, you can control whether it takes over
	12.1(13)EThe minimum deThe delay periodIf the active routernew active routeras the active routerHowever, even ifactive role after ito set a delay perthrough before thWe recommend t	Support for this command was introduced on the MSFC. lay period applies to all subsequent interface events. applies only to the first interface-up event after the router has reloaded. er fails or is removed from the network, the standby router automatically becomes the : If the former active router comes back online, you can control whether it takes over er by using the standby preempt command. the standby preempt command is not configured, the former active router resumes the t reloads and comes back online. Use the standby delay minimum reload command iod for HSRP group initialization. This command allows time for the packets to get
	12.1(13)EThe minimum deThe delay periodIf the active routernew active routeras the active routeras the active routHowever, even ifactive role after ito set a delay perthrough before thWe recommend ticommand is configuration	Support for this command was introduced on the MSFC. lay period applies to all subsequent interface events. applies only to the first interface-up event after the router has reloaded. er fails or is removed from the network, the standby router automatically becomes the . If the former active router comes back online, you can control whether it takes over er by using the standby preempt command. the standby preempt command is not configured, the former active router resumes the t reloads and comes back online. Use the standby delay minimum reload command iod for HSRP group initialization. This command allows time for the packets to get the router resumes the active role. hat you use the standby delay minimum reload command if the standby timers

Examples	This example shows how to set the minimum delay period to 30 seconds and the delay period after the first reload to 120 seconds:
	Router(config-if) # standby delay minimum 30 reload 120 Router(config-if) #

Related Commands show standby delay

standby delay minimum reload (refer to Cisco IOS documentation)
standby preempt (refer to Cisco IOS documentation)
standby timers (refer to Cisco IOS documentation)

standby ip

To enable HSRP and set the virtual IP address, use the **standby ip** command. Use the **no** form of this command to disable HSRP.

standby [group-number] ip [ip-addr [secondary]]

no standby [group-number] **ip** [ip-addr]

Syntax Description	group-number	(Optional) Group number on the interface for which HSRP is being activated; valid values are from 0 to 255.	
	ip-addr	(Optional) IP address of the Hot Standby router interface.	
	secondary	(Optional) Specifies a secondary virtual IP address.	
Defaults	The defaults are as	s follows:	
	• HSRP is disabled		
	• group-number—If you do not specify a group-number, group 0 is used		
	 priority—10 		
	• <i>delay</i> — 0		
	• hellotime—3 seconds		
	 <i>holdtime</i>—10 seconds 		
Command Modes	Interface configur	Modification	
ooniniana motor j	12.1E	Support for this command was introduced on the MSFC.	
Usage Guidelines	The standby ip command activates HSRP on the configured interface. If an IP address is specified, that address is used as the designated address for the Hot Standby group. If no IP address is specified, the designated address is learned through the standby function. For HSRP to elect a designated router, at		
		the cable must have been configured with, or have learned, the designated address. esignated address on the active router always overrides a designated address that is	
	changed (unless pr requests are answe	v ip command is enabled on an interface, the handling of proxy ARP requests is roxy ARP was disabled). If the Hot Standby state of the interface is active, proxy ARP ered using the MAC address of the Hot Standby group. If the interface is in a different responses are suppressed.	
	When group numb compatibility.	ber 0 is used, no group number is written to NVRAM, providing backward	

To assist in troubleshooting, configure the group-number to match the VLAN number.

Increase the *priority* of at least one interface in the HSRP group. The interface with the highest priority becomes active for that HSRP group.

All interfaces in the HSRP group should use the same timer values.

All interfaces in the HSRP group should use the same authentication string.

The alt keyword is used to specify an alternate configuration and is used in the following:

- [no] standby [group-number] ip [ip-address [secondary]] alt [no] standby [group-number] ip
 [ip-address [secondary]]
- [no] standby [group-number] priority priority [preempt [delay delay]] alt [no] standby [group-number] priority priority [preempt [delay delay]]

For additional information, see the "alt Keyword Usage" section on page 2-9.

Examples

This example shows how to enable HSRP for group 1 on an interface. The IP address used by the Hot Standby group will be learned using HSRP.

Router(config-if) # standby 1 ip
Router(config-if) #

standby track

To configure an interface so that the Hot Standby priority changes are based on the availability of other interfaces, use the **standby track** command. Use the **no standby** *group-number* **track** command to delete all tracking configuration for a group.

standby [group-number] **track** {*interface-type interface-number* | **designated-router**} [priority-decrement]

no standby group-number track

group	(Optional) Specifies the group number on the interface to which the tracking applies; valid values are from 0 to 255.	
interface-type interface-number	Specifies the interface type and number to be tracked.	
designated-router	Specifies that if the designated router becomes nondesignated, the active HSRP router becomes the designated router.	
priority-decrement	(Optional) Specifies the amount that the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up); valid values are from 1 to 255.	
The defaults are as f	follows:	
• The group is 0 .		
• The <i>priority-decrement</i> is 10 .		
• The designated-router option is disabled.		
Interface configurati	Modification	
	This command was introduced on the MSFC2.	
	This command was changed to include the designated-router option.	
This command is sup on systems configur Prior to entering the higher HSRP priorit When a tracked inter	opported on systems configured with an MSFC2 only. This command is not supported	
	interface-type interface-number designated-router priority-decrement The defaults are as f • The group is 0. • The priority-dec • The designated Interface configurat: Release 12.1(14)E 12.1(13.05)E0 This command is sup on systems configur Prior to entering the higher HSRP priorit	

When multiple tracked interfaces are down, the decrements are cumulative whether they are configured with priority-decrement values or not. A tracked interface is considered down if the IP address is disabled on that interface. You must enter the group-number when using the no form of this command. If you configure HSRP to track an interface, and that interface is physically removed as in the case of an OIR operation, then HSRP regards the interface as always down. You cannot remove the HSRP interface tracking configuration. To prevent this situation, use the **no standby track** interface-type interface-number command before you physically remove the interface. When you enter a group-number **0**, no group number is written to NVRAM, providing backward compatibility. Examples This example shows how to enable HSRP tracking for group 1 on an interface: Router(config-if)# standby 1 track Ethernet0/2 Router(config-if)# This example shows how to specify that if the designated router becomes nondesignated, the active HSRP router becomes the designated router: Router(config-if) # standby 1 track designated-router 15 Router(config-if)#

Related Commands show standby (refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference*)

upgrade rom-monitor

To set the execution preference on a ROMMON, use the **upgrade rom-monitor** command.

 $upgrade\ rom-monitor\ \{\{rp\ |\ sp\}\ \{invalidate\ |\ preference\}\ \{region1\ |\ region2\}$

upgrade rom-monitor {{**rp** | **sp**} **file** {*device:filename*}

Syntax Description	rp	Specifies the route processor.
	sp	Specifies the Catalyst 6500 series switch processor.
	invalidate	Invalidates the MAGIC and sequence code of the selected region.
	preference	Sets the execution preference on a ROMMON to the selected region.
	region1	Selects the ROMMON in region 1.
	region2	Selects the ROMMON in region 2.
	file	Specifies the name of the Flash file.
	device:filename	Name of the device and filename of the Flash file.

Defaults

This command has no default settings.

Command ModesPrivileged EXEC

Command History	Release	Modification
	12.1E	This command was introduced on the MSFC.
	12.1(3a)E1	Initial support of the MSFC2 on the Supervisor Engine 2.

Usage Guidelines

```
<u>A</u>
Caution
```

If you enter the **upgrade rom-monitor** command with no parameters, service may be interrupted.

Caution

If you enter the **upgrade rom-monitor** command from a Telnet session instead of a console connection, service may be interrupted.

	Note	Releases 12.1(8a)EX and earlier do not support the field-upgradable ROMMON feature on a Supervisor Engine 2. If you revert to a release prior to 12.1(8a)EX on a Supervisor Engine 2, the previously upgraded ROMMON will be invalidated and returned to run the ROMMON stored on the PROM. If you wish to use releases prior to 12.1(8a)EX on a Supervisor Engine 2, but upgrade your ROMMON, you must physically replace a ROMMON PROM with a ROMMON PROM that is programmed with the new ROMMON image. Contact Cisco TAC for additional information.		
		The slot <i>num</i> is required for this command to function properly.		
	The sp keyword is not supported.			
		You can enter the upgrade rom-monitor rp { invalidate preference } { region1 region2 } command to manually set the execution preference on a ROMMON in region1 or region2. This command is entered in EXEC privileged mode only.		
		You can enter the upgrade rom-monitor rp file { <i>device:filename</i> } command to program a new ROMMON into a FLASH (region1 or region2) region.		
Examples		This example shows how to program the new ROMMON into the MSFC2 ROMMON flash file:		
		Router# upgrade rom-monitor rp file bootflash:FUR_173.srec ROMMON image upgrade in progress Erasing flash Programming flash Verifying new image ROMMON image upgrade complete, MSFC2 must be reloaded.		

Related Commandsshow msfc2 rom-monitor



Acronyms

Table A-1 defines the acronyms used in this publication.

Table A-1List of Acronyms

Acronym	Expansion
AAL	ATM adaptation layer
ACE	access control entry
ACL	access control list
ACNS	Application and Content Networking System
AFI	authority and format identifier
Agport	aggregation port
ALPS	Airline Protocol Support
AMP	Active Monitor Present
APaRT	Automated Packet Recognition and Translation
ARP	Address Resolution Protocol
ATA	Analog Telephone Adaptor
ATM	Asynchronous Transfer Mode
AV	attribute value
BDD	binary decision diagrams
BECN	backward explicit congestion notification
BGP	Border Gateway Protocol
BPDU	bridge protocol data unit
BRF	bridge relay function
BSC	Bisync
BSTUN	Block Serial Tunnel
BUS	broadcast and unknown server
BVI	bridge-group virtual interface
CAM	content-addressable memory
CAR	committed access rate
CBAC	context based access control

Acronym	Expansion
CCA	circuit card assembly
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
СНАР	Challenge Handshake Authentication Protocol
CIR	committed information rate
CIST	Common and Internal Spanning Tree
CLI	command-line interface
CLNS	Connection-Less Network Service
CMNS	Connection-Mode Network Service
COPS	Common Open Policy Server
COPS-DS	Common Open Policy Server Differentiated Services
CoS	class of service
CPLD	Complex Programmable Logic Device
CRC	cyclic redundancy check
CRF	concentrator relay function
CST	Common Spanning Tree
CUDD	University of Colorado Decision Diagram
DCC	Data Country Code
dCEF	distributed Cisco Express Forwarding
DDR	dial-on-demand routing
DE	discard eligibility
DEC	Digital Equipment Corporation
DFC	Distributed Forwarding Card
DFI	Domain-Specific Part Format Identifier
DFP	Dynamic Feedback Protocol
DISL	Dynamic Inter-Switch Link
DLC	Data Link Control
DLSw	Data Link Switching
DMP	data movement processor
DNS	Domain Name System
DoD	Department of Defense
DOS	denial of service
dot1q	802.1Q
dot1x	802.1x
DRAM	dynamic RAM

Table A-1 List of Acronyms (continued)

Acronym	Expansion
DSAP	destination service access point
DSCP	differentiated services code point
DSPU	downstream SNA Physical Units
DSTS	Destination-Specific Traffic-Shaping
DTP	Dynamic Trunking Protocol
DTR	data terminal ready
DXI	data exchange interface
EAP	Extensible Authentication Protocol
EARL	Enhanced Address Recognition Logic
EEPROM	electrically erasable programmable read-only memory
EHSA	enhanced high system availability
EIA	Electronic Industries Association
ELAN	Emulated Local Area Network
EOBC	Ethernet out-of-band channel
EOF	end of file
EoMPLS	Ethernet over Multiprotocol Label Switching
ESI	end-system identifier
FAT	File Allocation Table
FECN	forward explicit congestion notification
FIB	Forwarding Information Base
FM	feature manager
FRU	field replaceable unit
fsck	file system consistency check
FSM	feasible successor metrics
FSU	fast software upgrade
GARP	General Attribute Registration Protocol
GBIC	Gigabit Interface Converter
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HSRP	Hot Standby Routing Protocol
ICC	Inter-card Communication or interface controller card
ICD	International Code Designator
ICMP	Internet Control Message Protocol
IDB	interface descriptor block
IDP	initial domain part or Internet Datagram Protocol
IDSM	Intrusion Detection System Module

Table A-1 List of Acronyms (continued)

Acronym	Expansion
IFS	IOS File System
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IP	Internet Protocol
IPC	interprocessor communication
IPX	Internetwork Packet Exchange
IS-IS	Intermediate System-to-Intermediate System Intradomain Routing Protocol
ISL	Inter-Switch Link
ISL VLANs	Inter-Switch Link VLANs
ISO	International Organization of Standardization
ISR	Integrated SONET router
LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol data unit
LAN	local area network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LCP	Link Control Protocol
LDA	Local Director Acceleration
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LEM	link error monitor
LER	link error rate
LES	LAN Emulation Server
LLC	Logical Link Control
LTL	Local Target Logic
MAC	Media Access Control
MD5	message digest 5
MFD	multicast fast drop
MIB	Management Information Base
MII	media-independent interface
MLS	Multilayer Switching
MLSE	maintenance loop signaling entity
МОР	Maintenance Operation Protocol
MOTD	message-of-the-day

Table A-1 List of Acronyms (continued)

Acronym	Expansion
MLSE	maintenance loops signaling entity
MPLS	Multiprotocol Label Switching
MRM	multicast routing monitor
MSDP	Multicast Source Discovery Protocol
MSFC	Multilayer Switching Feature Card
MSM	Multilayer Switch Module
MST	Multiple Spanning Tree (802.1s)
MTU	maximum transmission unit
MVAP	multiple VLAN access port
NAM	Network Analysis Module
NBP	Name Binding Protocol
NCIA	Native Client Interface Architecture
NDE	NetFlow Data Export
NET	network entity title
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card
NMP	Network Management Processor
NSAP	network service access point
NTP	Network Time Protocol
NVGEN	nonvolatile generation
NVRAM	nonvolatile RAM
OAM	Operation, Administration, and Maintenance
ODM	order dependent merge
OSI	Open System Interconnection
OSM	Optical Services Module
OSPF	open shortest path first
PAE	port access entity
PAgP	Port Aggregation Protocol
PBD	packet buffer daughterboard
PC	Personal Computer (formerly PCMCIA)
PCM	pulse code modulation
PCR	peak cell rate
PDP	policy decision point
PDU	protocol data unit
PEP	policy enforcement point

Table A-1 List of Acronyms (continued)

Acronym	Expansion
PGM	Pragmatic General Multicast
PHY	physical sublayer
PIB	policy information base
PIM	protocol independent multicast
PPP	Point-to-Point Protocol
PRID	Policy Rule Identifiers
PVLANs	private VLANs
PVST+	Per-VLAN Spanning Tree+
QDM	QoS device manager
QM	QoS manager
QM-SP	SP QoS manager
QoS	quality of service
Q-in-Q	802.1Q in 802.1Q
RACL	router interface access control list
RADIUS	Remote Access Dial-In User Service
RAM	random-access memory
RCP	Remote Copy Protocol
RF	Redundancy Facility
RGMP	Router-Ports Group Management Protocol
RIB	routing information base
RIF	Routing Information Field
RMON	remote network monitor
ROM	read-only memory
ROMMON	ROM monitor
RP	route processor or rendezvous point
RPC	remote procedure call
RPF	reverse path forwarding
RPR	Route Processor Redundancy
RPR+	Route Processor Redundancy+
RSPAN	remote SPAN
RST	reset
RSTP	Rapid Spanning Tree Protocol
RSTP+	Rapid Spanning Tree Protocol plus
RSVP	ReSerVation Protocol
SAID	Security Association Identifier
SAP	service access point

Table A-1 List of Acronyms (continued)

Acronym	Expansion
SCM	service connection manager
SCP	Switch-Module Configuration Protocol
SDLC	Synchronous Data Link Control
SGBP	Stack Group Bidding Protocol
SIMM	single in-line memory module
SLB	server load balancing
SLCP	Supervisor Line-Card Processor
SLIP	Serial Line Internet Protocol
SMDS	Software Management and Delivery Systems
SMF	software MAC filter
SMP	Standby Monitor Present
SMRP	Simple Multicast Routing Protocol
SMT	Station Management
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SREC	S-Record format, Motorola defined format for ROM contents
SSTP	Cisco Shared Spanning Tree
STP	Spanning Tree Protocol
SVC	switched virtual circuit
SVI	switched virtual interface
TACACS+	Terminal Access Controller Access Control System Plus
TARP	Target Identifier Address Resolution Protocol
ТСАМ	Ternary Content Addressable Memory
TCL	table contention level
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TopN	Utility that allows the user to analyze port traffic by reports
TOS	type of service
TLV	type-length-value
TTL	Time To Live
TVX	valid transmission
UDLD	UniDirectional Link Detection Protocol
UDP	User Datagram Protocol
UNI	User-Network Interface

Table A-1 List of Acronyms (continued)

Acronym	Expansion
UTC	Coordinated Universal Time
VACL	VLAN access control list
VCC	virtual channel circuit
VCI	virtual circuit identifier
VCR	Virtual Configuration Register
VINES	Virtual Network System
VLAN	virtual LAN
VMPS	VLAN Membership Policy Server
VPN	virtual private network
VRF	VPN routing and forwarding
VTP	VLAN Trunking Protocol
VVID	voice VLAN ID
WAN	wide area network
WCCP	Web Cache Coprocessor Protocol
WFQ	weighted fair queueing
WRED	weighted random early detection
WRR	weighted round-robin
XNS	Xerox Network System

Table A-1 List of Acronyms (continued)



Acknowledgments for Open-Source Software

The Cisco IOS software on the Catalyst 6500 series switches software pipe command uses Henry Spencer's regular expression library (regex).

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

- 1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
- 2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
- 3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
- 4. This notice may not be removed or altered.



Symbols

?

command completion 1-14 listing available commands 1-14 ? command 1-1

Numerics

802.3ad See LACP

Α

abbreviating commands 1-13 context-sensitive help 1-1 access control lists See ACLs accessing MSFC console port 1-11 Telnet session 1-12 ACLs merge displaying current method 2-51 selecting BDD-based merge method 2-28 ODM-based merge method 2-28 acronyms, list of A-1 addresses primary IP 2-10 secondary IP 2-10 Address Resolution Protocol See ARP

audience vii authentication proxy watch list adding IP address 2-13 clearing entries 2-2 configuring 2-13 disabling 2-13 displaying 2-54 enabling 2-13 setting maximum login attempts 2-12

В

BDD selecting ACL merge method 2-28 BGP configuring maximum number of parallel routes 2-27 creating traffic classification 2-43 binary decision diagrams See BDD boot field default values, changing 2-3 booting system software, configuration register 2-3 boot register 2-3 Border Gateway Protocol See BGP bridge crb command 2-11 bridge group command 2-11 bridge protocol data unit See BPDU bundled images displaying 2-59

С

CEF disabling rate-limiting 2-32 enabling rate-limiting 2-32 setting load balancing to include Layer 4 ports 2-31 rate-limiting 2-32 Cisco Express Forwarding See CEF CLI backing out one level 1-13 configuration mode 1-12 console configuration mode 1-13 getting list of commands 1-14 global configuration mode 1-13 interface configuration mode (IOS) 1-13 levels of access 1-12 MSFC CLI accessing 1-11 privileged EXEC mode 1-13 software basics 1-12 string search alternation 1-8 anchoring 1-8 expressions 1-5 filtering 1-5 multiple-character patterns 1-7 multipliers 1-7 parentheses for recall 1-9 searching outputs 1-5 single-character patterns 1-6 using 1-5 command execution multiple interfaces simultaneously 2-8 command-line interface See CLI

commands, getting list of 1-14 committed information rate See CIR configuration, saving 1-11 configuration mode 1-12 consistency checker configuring 2-37 disabling 2-37 enabling 2-37 console configuration mode 1-13 accessing 1-13 description 1-13 prompt 1-13 console port accessing MSFC 1-11

D

default form of a command, using 1-5 Distributed Forwarding Card See DFC document conventions viii document organization vii dot1q See 802.1Q tunneling dot1x See 802.1x

Е

enable mode 1-13 encapsulation IPX 2-23 Enhanced Address Recognition Logic See EARL Ethernet over Multiprotocol Label Switching See EoMPLS executing a command on multiple interfaces 2-8

expressions

matching multiple expression occurrences 1-7 multiple-character patterns 1-7 multiplying pattern occurrence 1-9 single-character patterns 1-6 specifying alternative patterns 1-8 extended networks

IP, using secondary addresses 2-11

F

fast software upgrade See FSU FDDI raw, IPX encapsulation 2-24 feature manager displaying CBAC-configured ACL lists and ports 2-47 dynamic reflexive entries 2-50 general information 2-44 inband packet count 2-46 per-interface information 2-48 per-VLAN information 2-52 summaries 2-51 field-replaceable unit See FRU file system consistency check See fsck fm See feature manager framing IPX See IPX, encapsulations

G

global configuration mode accessing 1-13 description 1-13 prompt 1-13

Н

hardware switching configuring consistency checker 2-37 disabling consistency checker 2-37 enabling consistency checker 2-37 Hot Standby Router Protocol See HSRP HSRP configuring initialization delay 2-71 tracking 2-75 disabling delay period 2-71 displaying delay period 2-71

I

ICMP subnet masks 2-10 informs, enabling 2-68 inter-card communication See ICC interface configuration mode accessing 1-13 description 1-13 prompt 1-13 interface-range macro creating 2-5 interfaces addresses, secondary 2-10 intermediate system-to-intermediate system See IS-IS Internet Control Message Protocol (ICMP) See ICMP entries Internet Group Management Protocol

See IGMP Internetwork Packet Exchange See IPX interprocessor communication See IPC Inter-Switch Link VLANs See ISL VLANs IOS bringing up interface 1-15 viewing and saving configuration 1-15 IP addresses primary 2-10 secondary 2-10 primary address, setting 2-10 secondary address, specifying 2-10 IP routing protocols configuring maximum number of parallel routes 2-27 **IP WCCP** disabling packet redirection on an interface 2-21 enabling packet redirection on an interface 2-21 IPX encapsulations 2-23 ARPA 2-24 Ethernet 802.2 2-24 Ethernet 802.3 2-24 Ethernet_II 2-24 Ethernet_Snap 2-24 FDDI raw 2-24 HDLC 2-24 Novell-Ether 2-24 SAP 2-24 SNAP 2-24 framing See IPX, encapsulations multiple logical networks 2-24 routing

disabling 2-23 enabling 2-23 enabling on multiple networks (example) 2-26 secondary networks 2-23 subinterfaces 2-24 configuration (example) 2-26

J

jumbo frames default value 2-40 restoring default value 2-40 setting maximum packet size 2-40 setting maximum transmission unit size 2-40

L

Layer 3 manager displaying information 2-57 LCP displaying bundled images 2-59 Link Aggregation Control Protocol See LACP

Μ

macro creating an interface-range macro 2-5 maintenance loop signaling entity See MLSE maximum transmission unit See MTU MCP displaying bundles images 2-59 Media Access Control See MAC address table message digest 5 See MD5

message-of-the-day See MOTD MLS displaying ACL merge method 2-51 MSFC command permitting traffic 2-35 selecting ACL merge method 2-28 MLS IP deleting ACL threshold 2-34 global disabling consistency checker 2-37 enabling consistency checker 2-37 installing ACL threshold 2-36 interface disabling internal router 2-30 enabling internal router 2-30 enabling non-RPF multicast fastdrop 2-39 more commands filter 1-5 search 1-5 --More-- prompt filter 1-5 search 1-5 MSFC accessing from supervisor engine console port 1-11 telnet session 1-12 configuration mode 1-14 programing new ROMMON into Flash 2-77 session command and 1-12 setting execution preference 2-77 supervisor engine console command 1-11 MSFC CLI accessing 1-11 MSFC commands interface range 2-8

mls ip inspect 2-35 set traffic-index 2-43 show microcode 2-59 show msfc2 rom-monitor 2-60 show scp 2-62 upgrade rom-monitor 2-77 MTU default values 2-40 restoring default value 2-40 setting maximum packet size 2-40 setting maximum size 2-40 Multilayer Switch Feature Card See MSFC Multilayer Switching See MLS multiple-character patterns 1-7 Multiple Spanning Tree See MST Multiprotocol Label Switching See MPLS

Ν

NetFlow Data Export See NDE network entity title See NET NLSP subinterfaces 2-24 configuration (example) 2-26 no form of a command, using 1-5 non-RPF multicast fastdrop enabling 2-39

0

ODM selecting ACL merge method 2-28

order-dependent merge algorithm See ODD

Ρ

paging prompt see -- More -- prompt parallel router 2-11 per-VLAN spanning tree See PVST+ PIM disabling triggered RPF check 2-16 setting back-off interval 2-16 setting check interval 2-18 setting triggered check interval 2-16 port range executing 2-8 primary address IP, setting 2-10 private VLANs See PVLANs privileged EXEC mode accessing 1-13 description 1-13 prompt 1-13 Protocol Independent Multicast See PIM

Q

Q-in-Q 802.1Q in 802.1Q See 802.1Q tunneling QoS Device Manager See QDM question command 1-1

R

Rapid Spanning Tree Protocol See RSTP Rapid Spanning Tree Protocol+ See RSTP+ redundancy displaying configuration information 2-61 related documentation vii remote procedure call See RPC remote SPAN See RSPAN **Reverse Path Forwarding** See RPF ROMMON displaying status 2-60 programing new ROMMON into Flash 2-77 setting execution preference 2-77 Route Processor Redundancy See RPR Route Processor Redundancy+ See RPR+ router, parallel 2-11 RPF disabling exists-only checks 2-19 disabling triggered check 2-16 enabling exists-only checks 2-19 setting check interval 2-18 setting PIM back-off interval 2-16 setting triggered check interval 2-16

S

saving configuration changes 1-11 SCP displaying information 2-62 secondary address, IP, using 2-10

secondary networks, IPX 2-23 server load balancing See SLB session command, MSFC and 1-12 show commands filter 1-5 search 1-5 single-character patterns special characters single-character patterns, table 1-6 SLB displaying inband packet count 2-46 slot0 displaying information 2-64 **SNMP** informs disabling 2-68 enabling 2-68 traps disabling 2-68 enabling 2-68 software configuration boot register 2-3 special characters anchoring, table 1-8 SP QoS manager See QM-SP stub enabling non-RPF multicast fastdrop 2-39 subinterfaces IPX 2-24 NLSP 2-24 configuring (example) 2-26 subnet masks, using ICMP 2-10 supervisor engine image displaying bundled images 2-59 Switch-Module Configuration Protocol See SCP

Т

Tab key command completion 1-1 table contention level See TCL tables characters with special meaning 1-6 default MTU values 2-40 show ip wccp web-cache detail command output fields 2-56 special characters multipliers, table 1-7 special characters used for anchoring 1-8 Telnet, accessing MSFC 1-12 Ternary Content Addressable Memory See TCAM tracking configuring designated router 2-75 traps, enabling 2-68

U

user EXEC mode accessing 1-13 description 1-13 prompt 1-13

V

VLAN access control lists See VACL

W

watch list adding IP address 2-13 clearing entries 2-2

Catalyst 6500 Series Switch MSFC Command Reference—Release 12.1(13)E

configuring 2-13 disabling 2-13 displaying 2-54 enabling 2-13 setting maximum login attempts 2-12 WCCP displaying global statistics 2-55 inband packet count 2-46 Web Cache Coprocessor Protocol See WCCP weighted random early detection See WRED weighted round robin See WRR