Cisco IOS Mobile Wireless Radio Access Networking Command Reference

July 2008

Americas 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: 408 527-0883

Cisco IOS Mobile Wireless Radio Access Networking Command Reference

About Cisco IOS and Cisco IOS XE Software Documentation

Last updated: August 6, 2008

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- Documentation Objectives, page i
- Audience, page i
- Documentation Conventions, page ii
- Documentation Organization, page iii
- Additional Resources and Documentation Feedback, page xi

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is i ntended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- Typographic Conventions, page ii
- Command Syntax Conventions, page ii
- Software Conventions, page iii
- Reader Alert Conventions, page iii

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:

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

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

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- Cisco IOS Documentation Set, page iv
- Cisco IOS Documentation on Cisco.com, page iv
- Configuration Guides, Command References, and Supplementary Resources, page v

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/all_release/all_mcl.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xi.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS AppleTalk Configuration Guide *Cisco IOS XE AppleTalk Configuration Guide* *Cisco IOS AppleTalk Command Reference*	AppleTalk protocol.
Cisco IOS Asynchronous Transfer Mode Configuration Guide *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Bridging and IBM Networking Configuration Guide *Cisco IOS Bridging Command Reference* *Cisco IOS IBM Networking Command Reference*	• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
Cisco IOS Broadband and DSL Configuration Guide *Cisco IOS XE Broadband and DSL Configuration Guide* *Cisco IOS Broadband and DSL Command Reference*	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
Cisco IOS Carrier Ethernet Configuration Guide *Cisco IOS Carrier Ethernet Command Reference*	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
Cisco IOS Configuration Fundamentals Configuration Guide *Cisco IOS XE Configuration Fundamentals Configuration Guide* *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
Cisco IOS DECnet Configuration Guide *Cisco IOS XE DECnet Configuration Guide* *Cisco IOS DECnet Command Reference*	DECnet protocol.
Cisco IOS Dial Technologies Configuration Guide *Cisco IOS XE Dial Technologies Configuration Guide* *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
Cisco IOS Flexible NetFlow Configuration Guide *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS H.323 Configuration Guide	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
Cisco IOS High Availability Configuration Guide *Cisco IOS XE High Availability Configuration Guide* *Cisco IOS High Availability Command Reference*	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
Cisco IOS Integrated Session Border Controller Command Reference	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
Cisco IOS Intelligent Service Gateway Configuration Guide *Cisco IOS Intelligent Service Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
Cisco IOS Interface and Hardware Component Configuration Guide *Cisco IOS XE Interface and Hardware Component Configuration Guide* *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
Cisco IOS IP Addressing Services Configuration Guide *Cisco IOS XE Addressing Services Configuration Guide* *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
Cisco IOS IP Application Services Configuration Guide *Cisco IOS XE IP Application Services Configuration Guide* *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
Cisco IOS IP Mobility Configuration Guide *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.
Cisco IOS IP Multicast Configuration Guide *Cisco IOS XE IP Multicast Configuration Guide* *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS IP Routing Protocols Configuration Guide *Cisco IOS XE IP Routing Protocols Configuration Guide* *Cisco IOS IP Routing Protocols Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
Cisco IOS IP SLAs Configuration Guide *Cisco IOS XE IP SLAs Configuration Guide* *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
Cisco IOS IP Switching Configuration Guide *Cisco IOS XE IP Switching Configuration Guide* *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
Cisco IOS IPv6 Configuration Guide *Cisco IOS XE IPv6 Configuration Guide* *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
Cisco IOS ISO CLNS Configuration Guide *Cisco IOS XE ISO CLNS Configuration Guide* *Cisco IOS ISO CLNS Command Reference*	ISO connectionless network service (CLNS).
Cisco IOS LAN Switching Configuration Guide *Cisco IOS XE LAN Switching Configuration Guide* *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
Cisco IOS Mobile Wireless Home Agent Configuration Guide *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Multiprotocol Label Switching Configuration Guide *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
Cisco IOS Multi-Topology Routing Configuration Guide *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
Cisco IOS NetFlow Configuration Guide *Cisco IOS XE NetFlow Configuration Guide* *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, export features.
Cisco IOS Network Management Configuration Guide *Cisco IOS XE Network Management Configuration Guide* *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
Cisco IOS Novell IPX Configuration Guide *Cisco IOS XE Novell IPX Configuration Guide* *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
Cisco IOS Optimized Edge Routing Configuration Guide *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
Cisco IOS Quality of Service Solutions Configuration Guide *Cisco IOS XE Quality of Service Solutions Configuration Guide* *Cisco IOS Quality of Service Solutions Command Reference*	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
Cisco IOS Security Configuration Guide *Cisco IOS XE Security Configuration Guide* *Cisco IOS Security Command Reference*	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Service Selection Gateway Configuration Guide *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.
Cisco IOS Software Activation Configuration Guide *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
Cisco IOS Software Modularity Installation and Configuration Guide *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
Cisco IOS Terminal Services Configuration Guide *Cisco IOS Terminal Services Command Reference* *Cisco IOS XE Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
Cisco IOS Virtual Switch Command Reference	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). **Note** For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
Cisco IOS Voice Configuration Library *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
Cisco IOS VPDN Configuration Guide *Cisco IOS XE VPDN Configuration Guide* *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
Cisco IOS Wide-Area Networking Configuration Guide *Cisco IOS XE Wide-Area Networking Configuration Guide* *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
Cisco IOS Wireless LAN Configuration Guide *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS Software System Messages	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last updated: August 6, 2008

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

- Initially Configuring a Device, page i
- Using the CLI, page ii
- Saving Changes to a Configuration, page xii
- Additional Information, page xii

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the "About Cisco IOS and Cisco IOS XE Software Documentation" document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

- Understanding Command Modes, page ii
- Using the Interactive Help Feature, page v
- Understanding Command Syntax, page vi
- Understanding Enable and Enable Secret Passwords, page viii
- Using the Command History Feature, page viii
- Abbreviating Commands, page ix
- Using Aliases for CLI Commands, page ix
- Using the no and default Forms of Commands, page x
- Using the debug Command, page x
- Filtering Output Using Output Modifiers, page x
- Understanding CLI Error Messages, page xi

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 1 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. Table 2 describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'.  If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

```
Router(config)# we<Tab> webvpn
```

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 3 describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, "two words" is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

  The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

Caution Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression "protocol."

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 5 shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at "^" marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- *Cisco IOS Release 12.2SR System Message Guide*
- *Cisco IOS System Messages, Volume 1 of 2* (Cisco IOS Release 12.4)
- *Cisco IOS System Messages, Volume 2 of 2* (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Using the Cisco IOS Command-Line Interface" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html

  or

  "Using Cisco IOS XE Software" chapter of the *Cisco ASR1000 Series Aggregation Services Routers Software Configuration Guide*:

  http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/using_cli.html
- Cisco Product Support Resources

  http://www.cisco.com/web/psa/products/index.html
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- *White Paper: Cisco IOS Reference Guide*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl\

Mobile Wireless Radio Access Networking Commands

clear ppp mux

To clear PPP mux statistics, use the **clear ppp mux** EXEC command.

clear ppp mux [**interface** *interface*]

Syntax Description

interface	(Optional) The identifier of the multilink or serial interface for which you want to clear counters.

Defaults

If no interface is specified, statistics for all multilink and serial interfaces are cleared.

Command Modes

EXEC

Command History

Release	Modification
12.2(8)MC2	This command was introduced.
12.2(15)MC1	This command was incorporated in Cisco IOS Release 12.2(15)MC1.
12.3(11)T	This command was incorporated in Cisco IOS Release 12.3(11)T.

Usage Guidelines

None

Examples

The following example clears PPP mux statistics for multilink interface 1:

```
clear ppp mux interface multilink1
```

Related Commands

Command	Description
show ppp mux	Displays PPP mux counters for the specified multilink interface.

ip rtp compression-connections (mobile wireless)

To specify the total number of Real-Time Transport Protocol (RTP) header compression connections that can exist on an interface, use the **ip rtp compression-connections** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip rtp compression-connections *number*

no ip rtp compression-connections

Syntax Description

number	Number of RTP header compression connections the cache supports, in the range from 3 to 1000.

Defaults

For PPP and High-Level Data Link Control (HDLC) interfaces, the default is 16 compression connections.

For Frame Relay interfaces, the default is 256 compression connections.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T and for PPP and HDLC interfaces, the maximum number of compression connections increased from 256 to 1000. For Frame Relay interfaces, the maximum number of compression connections increased from 32 to 256. The default number of compression connections was increased from 32 (fixed) to 256 (configurable).
12.1(4)E	This command was integrated into Cisco IOS Release 12.1(4)E and was supported on Cisco 7100 series routers.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.

Usage Guidelines

You should configure one connection for each RTP call through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.

Note Both ends of the serial connection must use the same number of cache entries.

Note The MGX-RPM-1FE-CP back card supports up to 150 RTP header compression connections on a T1 interface and up to 1000 connections per MLP bundle regardless of whether the bundle contains one T1 interface or four.

Examples

The following example changes the number of RTP header compression connections supported to 150:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression
Router(config-if)# ip rtp compression-connections 150
Router(config-if)# exit
```

Related Commands

Command	Description
ip rtp header-compression	Enables RTP header compression.
show ip rtp header-compression	Displays RTP header compression statistics.

ip rtp header-compression (mobile wireless)

To enable Real-Time Transport Protocol (RTP) header compression, use the **ip rtp header-compression** command in interface configuration mode. To disable RTP header compression, use the **no** form of this command.

ip rtp header-compression [**passive | iphc-format | ietf-format**] [**periodic-refresh**] **[ignore-id]**

no ip rtp header-compression [**passive | iphc-format | ietf-format**] [**periodic-refresh**] **[ignore-id]**

Syntax Description

passive	(Optional) Compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed. If you do not specify the **passive** keyword, all RTP packets are compressed. This option is not applicable on PPP links.
iphc-format	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
ietf-format	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used.
periodic-refresh	(Optional) Indicates that the compressed IP header will be refreshed periodically.
ignore-id	(Optional) Suppresses the IP ID checking in RTP/UDP header compression.

Defaults

Disabled

For PPP interfaces, the default format for header compression is the IPHC format.

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format for header compression is the original proprietary Cisco format. The maximum number of compression connections for the proprietary Cisco format is 256.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0	This command was integrated into Cisco IOS Release 12.0. The **iphc-format** optional keyword was added.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T and the **periodic-refresh** optional keyword was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and the **ietf-format** keyword was added.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and the mobile wireless-specific **ignore-id** optional keyword was added.

Usage Guidelines

You can compress IP/User Datagram Protocol (UDP)/RTP headers to reduce the size of your packets. Compressing headers is especially useful for RTP because RTP payload size can be as small as 20 bytes, and the uncompressed header is 40 bytes.

Header Compression passive Keyword

By default, the **ip rtp header-compression** command compresses outgoing RTP traffic. This command includes an optional **passive** keyword. If you specify the **passive** keyword, outgoing RTP traffic is compressed only if *incoming* RTP traffic on the *same* interface is compressed. If you do not specify the **passive** keyword, *all* RTP traffic is compressed.

For PPP interfaces, the **passive** keyword is ignored. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

Header Compression iphc-format Keyword

This command includes the **iphc-format** keyword. The **iphc-format** keyword indicates the type of header compression that will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, TCP header-compression is also enabled. For this reason, the **ip tcp header-compression** command appears in the output of the **show running-config** command. Since both RTP and TCP header compression are enabled, both UDP and TCP packets are compressed.

The **iphc-format** keyword includes checking whether the destination port number is even and in the ranges of 16385 to 32767 (for Cisco audio) or 49152 to 65535 (for Cisco video). Valid RTP packets that meet the criteria (that is, the port number is even and within the specified range) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

Note For Frame Relay interfaces, the **iphc-format** keyword is not available.

Header Compression ietf-format Keyword

This command includes the **ietf-format** keyword. The **ietf-format** keyword indicates the type of header compression that will be used. For HDLC interfaces, the ietf-format compresses only UDP packets. For PPP interfaces, when the **ietf-format** keyword is specified, TCP header-compression is also enabled. For this reason, the **ip tcp header-compression** command appears in the output of the **show running-config** command. Since both RTP and TCP header compression are enabled, both UDP and TCP packets are compressed.

However, with the **ietf-format** keyword, the requirement of checking whether a destination port number is in a specific range has been removed. Any even destination port number higher than 1024 can be used. Valid RTP packets that meet the criteria (that is, the port number is even and higher than 1024), are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

Note For Frame Relay interfaces, the **ietf-format** keyword is not available.

Support for Serial Lines

RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection.

Unicast or Multicast RTP Packets

This command can compress unicast or multicast RTP packets, and, hence, multicast backbone (MBONE) traffic can also be compressed over slow links. The compression scheme is beneficial only when you have small payload sizes, as in audio traffic.

Examples

The following example enables RTP header compression on the Serial1/0.0 subinterface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip rtp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# exit
```

The following example enables RTP header compression on the Serial2/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip rtp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression ietf-format
Router(config-if)# ip rtp compression-connections 20
Router(config-if)# exit
```

In the following example, RTP header compression is enabled on the Serial1/0.1 subinterface and the optional **periodic-refresh** keyword of the **ip rtp header-compression** command is specified:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.1
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format periodic-refresh
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# exit
```

Related Commands

Command	Description
clear ip rtp header-compression	Clears RTP header compression structures and statistics.
ip rtp compression-connections	Specifies the total number of RTP header compression connections that can exist on an interface.
show ip rtp header-compression	Displays RTP header compression statistics.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

mode y-cable

To access the command mode that allows you to manually control the relays on the VWIC card, use the **mode y-cable** command.

mode y-cable

Syntax Description

This command has no parameters, it invokes the y-cable mode.

Defaults

There are no default settings or behaviors.

Command Modes

Redundancy configuration

Command History

Release	Modification
12.2(8)MC2	This command was introduced.
12.2(15)MC1	This command was incorporated in Cisco IOS 12.2(15)MC1.
12.3(11)T	This command was incorporated in Cisco IOS 12.3(11)T.

Examples

The following example enables y-cable mode.

```
mode y-cable
```

Related Commands

Command	Description
standalone	Indicates whether the MWR 1941-DC router is being used as a standalone device and manually sets the relays.
standby use-interface	Designates a loopback interface as a health or revertive interface.
redundancy	Invokes redundancy mode.

ppp mux

To enable PPP multiplexing/demultiplexing, use the **ppp mux** command in interface configuration mode. To disable PPP multiplexing/demultiplexing, use the **no** form of this command.

ppp mux

no ppp mux

Syntax Description

This command has no parameters.

Defaults

PPP multiplexing/demultiplexing is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)MC1	This command was introduced (MGX-RPM-1FE-CP back card).
12.2(8)MC2	This command was introduced (MWR 1941-DC router).
12.3(11)T	This command was incorporated in Cisco IOS 12.3(11)T.

Examples

The following example enables PPP multiplexing/demultiplexing.

```
ppp mux
```

Related Commands

Command	Description
ppp mux delay	Sets the maximum delay.
ppp mux frame	Sets the maximum length of the PPP superframe.
ppp mux pid	Sets the default PPP protocol ID.
ppp mux subframe count	Sets the maximum number of subframes in a superframe.
ppp mux subframe length	Sets the maximum length of the PPP subframe.
show ppp mux	Displays PPP mux counters for the specified multilink interface.

ppp mux delay

To set the maximum time the processor can wait before sending a superframe, use the **ppp mux delay** command in interface configuration mode. To set the maximum delay to the default, use the **no** form of this command.

ppp mux delay ***integer***

no ppp mux delay

Syntax Description

integer	The maximum number of microseconds that the processor can wait before sending out a PPP superframe. Possible values: • Cisco MWR 1941-DC router—0 through 4000000 microseconds. • MGX-RPM-1FE-CP back card—1 through 4000000 microseconds.

Defaults

Cisco MWR 1941-DC router—The default maximum delay is 0, which indicates that a superframe will be sent when the transmit queue is full.

MGX-RPM-1FE-CP back card—The default maximum delay is 800.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)MC1	This command was introduced (MGX-RPM-1FE-CP back card).
12.2(8)MC2	This command was introduced (MWR 1941-DC router).
12.3(11)T	This command was incorporated in Cisco IOS 12.3(11)T.

Usage Guidelines

To use this command, you must first enable PPP multiplexing/demultiplexing.

MGX-RPM-1FE-CP Back Card

When the ppp mux delay command is configured, the maximum number of microseconds that the processor can wait resolves to the nearest 200-microsecond increment. For example, if ppp mux delay 302 is specified, the actual maximum number of microseconds that the processor can wait before sending out a PPP superframe is 400. If ppp mux delay 298 is specified, the actual maximum number of microseconds that the processor can wait before sending out a PPP superframe is 200.

Examples

The following example sets the maximum delay to 5 microseconds on the MWR 1941-DC router.

```
ppp mux delay 5
```

The following example sets the maximum delay to 200 microseconds on the MGX-RPM-1FE-CP back card.

```
ppp mux delay 200
```

Related Commands

Command	Description
ppp mux	Enables PPP multiplexing/demultiplexing
ppp mux frame	Sets the maximum length of the PPP superframe.
ppp mux pid	Sets the default PPP protocol ID.
ppp mux subframe count	Sets the maximum number of subframes in a superframe.
ppp mux subframe length	Sets the maximum length of the PPP subframe.
show ppp mux	Displays PPP mux counters for the specified multilink interface.

ppp mux frame

To set the maximum length (in bytes) of the PPP superframes, use the **ppp mux frame** command in interface configuration mode. To set the maximum length to the default, use the **no** form of this command.

ppp mux frame *integer*

no ppp mux frame

Syntax Description

integer	The maximum number of bytes in any multiplexed PPP superframe. Possible values: • Cisco MWR 1941-DC router—1 through 512 bytes. • MGX-RPM-1FE-CP back card—0 through 512 bytes.

Defaults

The default maximum length is 197.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)MC1	This command was introduced (MGX-RPM-1FE-CP back card).
12.2(8)MC2	This command was introduced (MWR 1941-DC router).
12.3(11)T	This command was incorporated in Cisco IOS 12.3(11)T.

Usage Guidelines

To use this command, you must first enable PPP multiplexing/demultiplexing.

Examples

The following example sets the maximum superframe length to 80 bytes.

```
ppp mux frame 80
```

Related Commands

Command	Description
ppp mux	Enables PPP multiplexing/demultiplexing
ppp mux delay	Sets the maximum delay.
ppp mux pid	Sets the default PPP protocol ID.
ppp mux subframe count	Sets the maximum number of subframes in a superframe.
ppp mux subframe length	Sets the maximum length of the PPP subframe.
show ppp mux	Displays PPP mux counters for the specified multilink interface.

ppp mux pid

To set the default receiving PPP protocol ID, use the **ppp mux pid** command in interface configuration mode. To remove this configuration, use the **no** form of this command.

ppp mux pid ***integer***

no ppp mux pid

Syntax Description

integer	The default value of the PPP protocol ID. Possible values are 0 through 65534.

Defaults

The default is 33 (0x21), which is the IP protocol.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)MC1	This command was introduced (MGX-RPM-1FE-CP back card).
12.2(8)MC2	This command was introduced (MWR 1941-DC router).
12.3(11)T	This command was incorporated in Cisco IOS 12.3(11)T.

Usage Guidelines

To use this command, you must first enable PPP multiplexing/demultiplexing.

Examples

The following example sets the default PPP protocol ID to 8.

```
ppp mux pid 8
```

Related Commands

Command	Description
ppp mux	Enables PPP multiplexing/demultiplexing
ppp mux delay	Sets the maximum delay.
ppp mux frame	Sets the maximum length of the PPP superframe.
ppp mux subframe count	Sets the maximum number of subframes in a superframe.
ppp mux subframe length	Sets the maximum length of the PPP subframe.
show ppp mux	Displays PPP mux counters for the specified multilink interface.

ppp mux subframe count

To set the maximum number of PPP subframes that can be contained in a superframe, use the **ppp mux subframe count** command in interface configuration mode. To set the maximum number to the default, use the **no** form of this command.

ppp mux subframe count ***integer***

no ppp mux subframe count

Syntax Description

integer	The maximum number of subframes that can be contained in a superframe. Possible values are 1 through 15 bytes. Possible values: • Cisco MWR 1941-DC router—1 through 15 bytes. • MGX-RPM-1FE-CP back card—0 through 15 bytes.

Defaults

The default maximum is 15.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)MC1	This command was introduced (MGX-RPM-1FE-CP back card).
12.2(8)MC2	This command was introduced (MWR 1941-DC router).
12.3(11)T	This command was incorporated in Cisco IOS 12.3(11)T.

Usage Guidelines

To use this command, you must first enable PPP multiplexing/demultiplexing.

Examples

The following example sets the maximum subframe count to 20 bytes.

```
ppp mux subframe count 20
```

Related Commands

Command	Description
ppp mux	Enables PPP multiplexing/demultiplexing
ppp mux delay	Sets the maximum delay.
ppp mux frame	Sets the maximum length of the PPP superframe.
ppp mux pid	Sets the default PPP protocol ID.

Command	Description
ppp mux subframe length	Sets the maximum length of the PPP subframe.
show ppp mux	Displays PPP mux counters for the specified multilink interface.

ppp mux subframe length

To set the maximum length (in bytes) of the PPP subframes, use the **ppp mux subframe length** command in interface configuration mode. To set the maximum length to the default, use the **no** form of this command.

ppp mux subframe length *integer*

no ppp mux subframe length

Syntax Description

integer	The maximum number of bytes in any single subframe that is to be multiplexed. Possible values: • Cisco MWR 1941-DC router—1 through 512 bytes. • MGX-RPM-1FE-CP back card—0 through 512 bytes.

Defaults

The default maximum length is 195.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)MC2	This command was introduced.
12.3(11)T	This command was incorporated in Cisco IOS 12.3(11)T.

Usage Guidelines

To use this command, you must first enable PPP multiplexing/demultiplexing. The maximum length of the subframe should be the maximum length of the superframe minus the length of the L2 header.

Examples

The following example sets the maximum subframe length to 20 bytes.

```
ppp mux subframe length 20
```

Related Commands

Command	Description
ppp mux	Enables PPP multiplexing/demultiplexing
ppp mux delay	Sets the maximum delay.
ppp mux frame	Sets the maximum length of the PPP superframe.
ppp mux pid	Sets the default PPP protocol ID.
ppp mux subframe count	Sets the maximum number of subframes in a superframe.
show ppp mux	Displays PPP mux counters for the specified multilink interface.

redundancy

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
12.3(11)T	This command was implemented on the MWR 1900 MWR.
12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.
12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all of the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, INternetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

Examples

The following example enables redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example assigns the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Cisco 10000 Series Router

The following example configures two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-red)# linecard-group 1 y-cable
Router(config-red-lc)# member subslot 2/1 primary
Router(config-red-lc)# member subslot 2/0 secondary
```

Cisco 7600 Series Router

The following example shows how to enter the main CPU submode:

```
Router (config)# redundancy
Router (config-r)# main-cpu
Router (config-r-mc)#
```

Related Commands

Command	Description
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.

Command	Description
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers.

show ip rtp header-compression (mobile wireless)

To display Enhanced Compressed Real-Time Transport Protocol (CRTP) statistics, use the **show ip rtp header-compression** command in privileged EXEC mode.

show ip rtp header-compression [**detail**] [*interface-type interface-number*]

Syntax Description

detail	(Optional) Displays details of each connection.
interface-type interface-number	(Optional) The interface type and number.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.3(5)T and the command output was modified to include information related to the Distributed Compressed Real-Time Transport Protocol (dCRTP) feature.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and the command output was modified to include information related to the Enhanced Compressed Real-Time Transport Protocol (ECRTP) feature.

Usage Guidelines

The **detail** keyword is not available with the **show ip rtp header-compression** command on a Route Switch Processor (RSP). However, the **detail** keyword is available with the **show ip rtp header-compression** command on a Versatile Interface Processor (VIP). Enter the **show ip rtp header-compression** *interface-type interface-number* **detail** command on a VIP to retrieve detailed information regarding RTP header compression on a specific interface.

The **detail** keyword is also not supported with the **show ip rtp header-compression** command on a Cisco MWR 1941-DC router or a MGX-RPM-1FE-CP back card (Cisco IOS Mobile Wireless IP Radio Access Network [IP-RAN] implementation). If specified when the command is entered, the output is not displayed. Additionally, some of the field descriptions displayed by the **show ip rtp header-compression** command do not apply to the MWR 1941-DC router and MGX-RPM-1FE-CP back card.

Examples

The following example displays statistics from ECRTP on an interface:

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
  Interface Serial2/0 (compression on, IETF, ECRTP)
    Rcvd:    1473 total, 1452 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    1234 total, 1216 compressed, 0 status msgs, 379 not predicted
             41995 bytes saved, 24755 bytes sent
             2.69 efficiency improvement factor
    Connect: 16 rx slots, 16 tx slots,
             6 misses, 0 collisions, 0 negative cache hits, 13 free contexts
             99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip rtp header-compression Field Descriptions

Field	Description
Interface	Type and number of interface.
Rcvd	Received statistics described in subsequent fields.
total	Number of packets received on the interface.
compressed	Number of packets received with compressed headers.
errors	Number of errors.
status msgs	Number of resynchronization messages received from the peer.
dropped	Number of packets dropped.
buffer copies	Number of buffers that were copied.
buffer failures	Number of failures in allocating buffers.
Sent	Sent statistics described in subsequent fields.
total	Number of packets sent on the interface.
compressed	Number of packets sent with compressed headers.
status msgs	Number of resynchronization messages sent from the peer.
not predicted	Number of packets taking a non-optimal path through the compressor.
bytes saved	Total savings in bytes due to compression.
bytes sent	Total bytes sent after compression.
efficiency improvement factor	Compression efficiency.
Connect	Connect statistics described in subsequent fields.
rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
misses	Total number of misses.
collisions	Total number of collisions.
negative cache hits	Total number of negative cache hits.
free contexts	Number of available context resources.

Table 1 show ip rtp header-compression Field Descriptions (continued)

Field	Description
hit ratio	Percentage of received packets that have an associated context.
five minute miss rate	Number of new flows found per second averaged over the last five minutes.
max	Highest average rate of new flows reported.

Related Commands

Command	Description
ip rtp compression-connections	Specifies the total number of RTP header compression connections supported on the interface.
ip rtp header-compression	Enables RTP header compression.

show ppp mux

To display counters for a multilink interface, use the **show ppp mux** command in EXEC mode.

show ppp mux [interface ***interface*****]**

Syntax Description

interface *interface*	(Optional) The identifier of the multilink or serial interface for which you want to view counters.

Defaults

If no interface is specified, statistics for all multilink and serial interfaces are displayed.

Command Modes

EXEC

Command History

Release	Modification
12.2(8)MC1	This command was introduced (MGX-RPM-1FE-CP back card).
12.2(8)MC2	This command was introduced (MWR 1941-DC router).
12.3(11)T	This command was incorporated into Cisco IOS Release 12.3(11)T.

Usage Guidelines

This command is only valid when issued against multilink or PPP interfaces.

Examples

The following is an example of the output generated by this command.

```
show ppp mux interface multilink 1

PPP Multiplex Statistics on Interface Multilink1:

Multiplex:
 Total input packets:0
 Errored input packets:0
 Valid input bytes:0
 Total output packets:0
 Multiplexed output packets:0
 Output bytes:0
 Efficiency improvement factor:0%

Demultiplex:
 Total input packets:0
 Multiplexed input packets:0
 Errored input packets:0
 Valid input bytes:0
 Total output packets:0
 Output bytes:0
 Efficiency improvement factor:0%
```

Table 2 describes the significant fields shown in the display.

Table 2 show ppp mux Field Descriptions

Field	Description
Total output packets	Number of outbound packets
Multiplexed output packets	Number of outbound multiplexed superframes
Output byte count	Number of outbound bytes
Total input packets	Number of inbound packets
Errored input packets	Number of inbound packets discarded due to error
Efficiency improvement factor	Percentage of efficiency improvement achieved through multiplexing or demultiplexing

The efficiency improvement factor is calculated as follows:

Multiplex efficiency improvement factor = 100 * (Total bytes saved) / (Total bytes received)

Where total bytes saved = bytes_received_at_muxer - bytes_sent_at_muxer.

Demultiplex efficiency improvement factor = 100 * (Total bytes saved) / (Total bytes sent)

Where total bytes saved = bytes_sent_at_demuxer - bytes_received_at_demuxer.

Related Commands

Command	Description
ppp mux	Enables PPP multiplexing/demultiplexing

standalone

To specify that the MWR 1941-DC is being used in a stand-alone configuration (which impacts the relays on the VWIC), use the **standalone** command. To use the MWR 1941-DC in a redundant configuration, use the **no** form of this command.

[**no**] **standalone**

Syntax Description

This command has no attributes.

Defaults

By default, the MWR 1941-DC is configured to be used in a redundant configuration (**no standalone**) and the relays are open.

Command Modes

Y-cable configuration

Command History

Release	Modification
12.2(8)MC2	This command was introduced.
12.3(11)T	This command was incorporated in Cisco IOS Release 12.3(11)T.

Usage Guidelines

Issuing the standalone command closes the relays on the VWICs installed in the MWR 1941-DC.

Examples

The following example closes the relays so that the MWR 1941-DC can be used as a stand-alone device.

```
standalone
```

Related Commands

Command	Description
mode y-cable	Invokes y-cable mode.
standby use-interface	Specifies the interfaces to be used for health and revertive interfaces.

standby use-interface

To designate a loopback interface as a health or revertive interface, use the **standby use-interface** command.

standby use-interface *interface* {**health | revertive | backhaul**}

Syntax Description

interface	Indicates the interface to be used with the specified parameter. For **health** and **revertive**, this is the loopback interface specified in the **standby track** command. For **backhaul**, the interface must be an MLPPP interface. If you want to use a serial interface as the backhaul, you must first configure that interface to be part of an MLPPP bundle.
health	Indicates the interface to monitor for an over temperature condition, the state of the processor, and the state of the T1/E1 firmware. If any of these watched conditions indicate a failure, this interface is brought down. Otherwise, the health interface remains in the up state.
revertive	Indicates the interface that acts as the revertive interface. If the MWR 1941-DC router changes state from active to standby, the revertive interface is brought up. If the MWR 1941-DC router changes state from standby to active, the revertive interface is brought down.
backhaul	Indicates the interface to be used for backhauling.

Defaults

By default, the MWR 1941-DC is configured to be used in a redundant configuration (**no standalone**) and the relays are open.

Command Modes

Y-cable configuration

Command History

Release	Modification
12.2(8)MC2	This command was introduced.
12.3(11)T	This command was incorporated in Cisco IOS Release 12.3(11)T.

Usage Guidelines

The loopback interfaces that you specify for health and revertive interfaces must be the same loopback interfaces that you specified in the **standby track** command. In the **standby track** command, the decrement value for the revertive interface should always be less than that for other interfaces. We recommend that you use loopback101 for health and loopback102 for revertive.

The interface that you specify for the backhaul must be an MLPPP interface. If you want to use a serial interface as the backhaul, you must first configure that interface to be part of an MLPPP bundle. We recommend you use multilink1 for the backhaul interface.

Examples

The following example specifies loopback101 as the health interface and loopback102 as the revertive interface.

```
standby use-interface loopback101 health
standby use-interface loopback102 revertive
standby use-interface multilink1 backhaul
```

Related Commands

Command	Description
mode y-cable	Invokes y-cable mode.
redundancy	Invokes redundancy mode.
standalone	Specifies whether the MWR 1941-DC router is used in a redundant or stand-alone configuration.
standby	Sets HSRP attributes