Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide

Release 12.4

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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide

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.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

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\

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco MWR 1941-DC Router with the Cisco IOS IP-RAN Feature Set

FThe functionality of the MWR 1941-DC router is dependent on the Cisco IOS image running on it. This document describes configuring the MWR 1941-DC router with the Cisco IOS IP-RAN feature set (software image).

For additional configuration topics, refer to the Cisco IOS configuration guide and command reference publications. These publications are available on the Documentation CD-ROM that came with your router, on the World Wide Web from Cisco's home page, or you can order printed copies separately.

This document contains the following sections:

- Feature Overview, page 2
- Configuring Tasks, page 8
- Monitoring and Maintaining the MWR 1941-DC Router, page 37
- Enabling Remote Management of the MWR 1941-DC Router, page 38
- Related Documentation, page 39

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

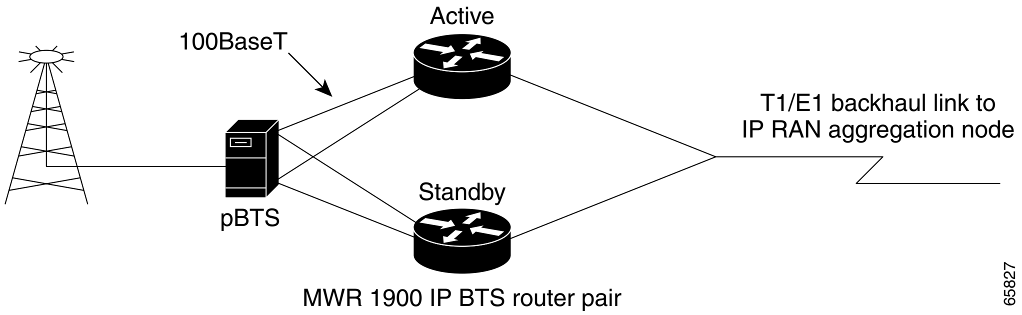
Feature Overview

In an IP RAN application, the Cisco MWR 1941-DC router extends IP connectivity to the cell site and Base Transceiver Station (BTS).

Through a FastEthernet interface to the BTS, the MWR 1941-DC router provides bandwidth-efficient IP transport of voice and data bearer traffic, as well as maintenance, control, and signalling traffic, over the leased line backhaul network between the BTS and leased line termination and aggregation node via compression (cRTP/cUDP) and packet multiplexing (PPPmux and MLPPP).

Figure 1 shows the placement of and connections for the MWR 1941-DC router implemented in an IP-RAN.

Figure 1 MWR 1941-DC Router in an IP-RAN Solution



In the IP-RAN, the BTS site consists of a pair of MWR 1941-DC routers. The pair of MWR 1941-DC routers provides for an active and standby router for redundancy. A failure of the active MWR 1941-DC router causes the standby router to take over as the active router for the BTS site.

Each pair of MWR 1941-DC routers at the BTS site is identical in hardware configuration. They connect to each other through the BTS via the Fast Ethernet interfaces. The individual backhaul links to an MWR 1941-DC router are cabled from a single T1/E1 termination block in the BTS, connecting to both the active and standby routers utilizing a “Y” cable. The redundancy design to control the active/standby transitions of the router pair leverages HSRP to control the relays on the VWIC-2MFT-T1-DIR (or VWIC-2MFT-E1-DIR) in each router to ensure that the relays on the active router are closed and the relays on the standby router are open to avoid double termination of the T1 (or E1).

Software Features with the Cisco IOS IP-RAN Feature Set

The software required for implementing the MWR 1941-DC router in an IP-RAN consists of two components: Cisco IOS software running on the MIPs-based route processor portion of the MWR 1941-DC router hardware, and microcode running on the Cisco network processor, also known as “Parallel eXpress Forwarding (PXF).” When deployed in an IP-RAN, the MWR 1941-DC router is customized for performance, high availability, quality of service, and link efficiency.

Cisco IOS software functions added to the MWR 1941-DC router IP-RAN feature set include:

- Redundancy logic—For monitoring Hot Standby Routing Protocol (HSRP) information to determine the active and standby router and control T1 termination.
- Failover logic—To force a switchover for hardware failures or an over-temperature condition.
- Relay control—To open and close the T1/E1 interfaces on the active and standby routers.
- Diagnostic functions—To monitor the “health” of the standby MWR 1941-DC router.

This section contains the following information:

- MIPs-Based Software Features, page 3
- Network Processor (PXF) Software Features, page 3
- Redundancy Support, page 5

MIPs-Based Software Features

Standard Cisco IOS software features supported in the MWR 1914-DC IP-RAN feature set include:

- IP Fragmentation
- IP Multicast
- IGMP
- MLP, PPP Control Path (IPCP, NCP, LCP, CLNS)
- ACFC and PFC Handling During PPP Negotiation
- HSRP
- OSPF
- DHCP
- CDP
- NTP
- SNMP

Network Processor (PXF) Software Features

To achieve the required efficiency, when implemented in an IP-RAN, the MWR 1941-DC router additionally has microcode running on the network processor to offload the fast-path processing of packets. This allows the MWR 1941-DC router to support the traffic of up to 4 T1s or E1s (up to 60,000 packets per second) at a targeted 80% processor utilization while performing UDP/RTP header compression/decompression (cUDP/cRTP) and PPPmux.

The following features are supported in the network processor:

- MAC Classify
- ICMP
- FIB (CEF)
- Load-balancing
- MAC Rewrite
- QoS Matching, including IP Access Lists (Input/Output Security ACLs are not supported), QoS Group, IP Precedence, IP DSCP, and Input Interface
- QoS Actions, including Set IP Precedence, Set IP DSCP, Set QoS Group, Traffic Shaping, Class Based WFQ (CB-WFQ), and Low Latency Queuing (LLQ)
- Maintenance of statistics, such as Forwarding, Drop, and Interface
- IPv4
- MLPPP, MLP, PPP Data Path (MLP LFI is not supported)
- PPPmux

- cRTP/cUDP
- Link Noise Monitoring (LNM) provides configuration monitoring of individual T1/E1 circuit quality

PPP Multiplexing/Demultiplexing

Encapsulated PPP frames contain several bytes of header information, which adds overhead to a network that is used to transport PPP frames.

RFC 3153 describes a way to overcome this overhead. On the sending end, a multiplexor concatenates multiple PPP frames (subframes) into a single, multiplexed frame (superframe). One header is included in the superframe and the individual PPP subframes are separated by delimiters. On the receiving end, a demultiplexor uses the delimiters to separate the individual PPP subframes.

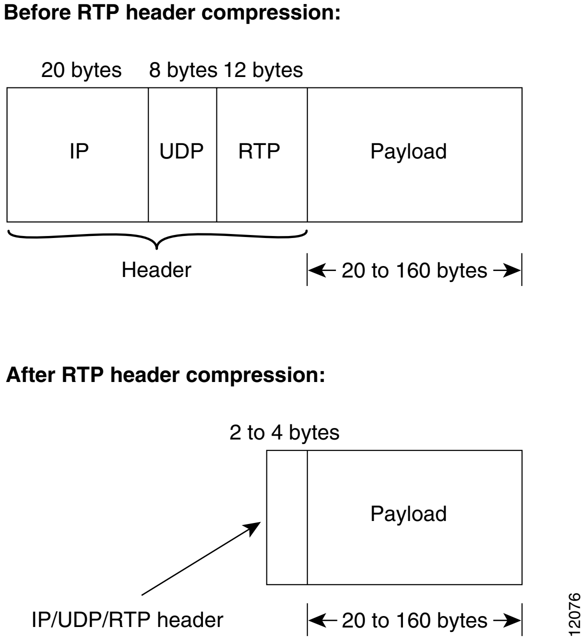
The MWR 1914-DC router network processor software conforms to this specification and acts as both a multiplexor and a demultiplexor.

RTP/UDP Header Compression

RTP is a protocol used for carrying packetized audio and video traffic over an IP network. RTP, described in RFC 1889, is not intended for data traffic, which uses TCP or UDP. Instead, RTP provides end-to-end network transport functions intended for applications with real-time requirements (such as audio, video, or simulation data) over multicast or unicast network services.

In an RTP frame, there is a minimum 12 bytes of the RTP header, combined with 20 bytes of IP header, and 8 bytes of UDP header. This creates a 40-byte IP/UDP/RTP header. By comparison, the RTP packet has a payload of approximately 20 to 160 bytes for audio applications that use compressed payloads. Given this ratio, it is very inefficient to transmit the IP/UDP/RTP header without compressing it.

Figure 2 RTP Header Compression



RFCs 2508 and 2509 describe a method for compressing not only the RTP header, but also the associated UDP and IP headers. Using this method, the 40 bytes of header information is compressed into approximately 2 to 4 bytes, as shown in Figure 2. Because the frames are compressed on a link-by-link basis, the delay and loss rate are lower, resulting in improved performance.

The MWR 1914-DC router network processor offloads both the compression and decompression of RTP frames from the Cisco IOS software.

Note The MWR 1941-DC router can be configured to perform only IP/UDP compression, in which case the header is reduced from 28 bytes to 2 to 4 bytes.

Redundancy Support

In an IP-RAN application, to ensure availability, the backhaul links to an MWR 1941-DC router are redundantly cabled to the VWIC-2MFT-T1-DIR/ VWIC-2MFT-E1-DIR cards. This card, designed specifically for the MWR 1941-DC router, is a modified 2-port T1/E1 Multiflex VWIC with Drop and Insert.The modifications include the addition of relays to activate the T1/E1 ports. The relays allow “Y” cabling for router redundancy where the T1/E1 link is not redundant and default to open. The relays are controlled by HSRP/redundancy protocol between the two routers connected to the same T1/E1.

Note If you choose to use the MWR 1941-DC router in a non-redundant configuration, you must close the relays on the card using the **standalone** subcommand. Also, redundancy parameters are processed when the router is booted up. These parameters cannot be changed “on the fly.”

HSRP

Cisco’s Hot Standby Router Protocol (HSRP) is used to control which router is active and which is standby. HSRP uses a priority scheme to determine which HSRP-configured router is to be the default active router. Priority is determined first by the configured priority value, and then by the IP address. In each case a higher value is of greater priority.

Supported MIBs

- CISCO-ACCESS-ENVMON-MIB
- CISCO-CDP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-HSRP-EXT-MIB
- CISCO-HSRP-MIB
- CISCO-ICSUDSU-MIB
- CISCO-IMAGE-MIB
- CISCO-IP-STAT-MIB

- CISCO-IPMROUTE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-MOBILE-IP-MIB
- CISCO-PROCESS-MIB
- CISCO-QUEUE-MIB
- CISCO-SYSLOG-MIB
- CISCO-TCP-MIB
- ENTITY-MIB
- IF-MIB
- IGMP-MIB
- IPMROUTE-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1253-MIB
- RFC1406-MIB
- TCP-MIB
- UDP-MIB

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

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

Note The MWR 1914-DC router uses the same software base as the Cisco 10000. As such, it shares the same QoS MIB limitations of the Cisco 10000. For information about the Cisco10000 MIB support, see the *Cisco 10000 Series ESR MIB Specifications Guide on CCO* at http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10kmibs/specgdll/index.htm.

Limitations and Restrictions

⚠ **Caution** The Cisco MWR 1941-DC router does not support online insertion and removal (OIR) of WAN interface cards. Any attempt to perform OIR on a card in a powered up router might cause damage to the card.

⚠ **Caution** Removing the compact flash from the Cisco MWR 1941-DC router during a read/write operation might corrupt the contents of the compact flash, rendering it useless. To recover from an accidental removal of or corruption to the compact flash, a maintenance spare with the appropriate bootable Cisco IOS software image might be needed.

The following list of restrictions applies when implementing the MWR 1941-DC router in an IP-RAN.

Cisco IOS Software Features not Supported on the MWR 1941-DC Router

The Cisco MWR 1941-DC router requires a special version of Cisco IOS software. Not all Cisco IOS software features can be used with the Cisco MWR 1941-DC router as the core routing is handled by the network processor. A list of supported features is included in the "Software Features with the Cisco IOS IP-RAN Feature Set" section on page 2. The following standard Cisco IOS software features are not supported on the Cisco MWR 1941-DC router:

- Security Access Control Lists
- MPLS
- 802.1Q VLANs
- Frame Relay (FR)
- MLP LFI
- ATM
- Use of additional WICs. The only supported WIC is the VWIC-2MFT-T1DIR/VWIC-2MFT-E1DIR. (IP-RAN implementation only.)

Upgrading the VWIC-2MFT-T1-DIR Microcode

When upgrading the image on your Cisco MWR 1941-DC router, power cycle the router or perform a microcode reload on the VWIC-2MFT-T1-DIR to ensure that the firmware for the VWIC-2MFT-T1-DIR is updated during the upgrade.

Disabling PPP Multiplexing

To fully disable PPP multiplexing (PPPMux), issue the **no ppp mux** command on the T1 interfaces of the routers at both ends of the T1 link. If PPP multiplexing remains configured on one side of the link, that side will offer to receive PPP multiplexed packets.

MLP LFI Support

MLP LFI is not supported by the Cisco MWR 1941-DC router. Therefore, MLP LFI must be disabled on peer devices connecting to the Cisco MWR 1941-DC router T1 MLP connections.

ACFC and PFC Support on PPP Interfaces

If upgrading to Cisco IOS Release 12.2(8)MC2c or later for the ACFC and PFC support on PPP interfaces, ensure that you upgrade the MGX-RPM-1FE-CP back card image first. After doing so, immediately upgrade all MWR 1941-DC routers connected to the MGX-RPM-1FE-CP back card.

Configuring Tasks

See the following sections for configuration tasks for configuring the Cisco MWR 1941-DC router in an IP-RAN.

- Before You Begin, page 8
- Slot and Port Numbering, page 9
- Verifying the Version of Cisco IOS Software, page 9
- Configuring the Host Name and Password, page 10
- Configuring Loopback Interfaces, page 11
- Configuring Fast Ethernet Interfaces, page 12
- Configuring Multilink Interfaces, page 17
- Configuring T1 and E1 Interfaces, page 23
- Configuring QoS Attributes, page 25
- Configuring Redundancy, page 28
- Configuring the Link Noise Monitor, page 30
- Saving the Configuration, page 33
- Verifying the Configuration, page 33

Before You Begin

Before you configure the MWR 1941-DC in an IP-RAN, please be aware of the following:

- Cisco IOS Release 12.2(8)MC2 or later "mwr1900-i-mz" image must be installed on the Cisco MWR 1941-DC router.
- You cannot disable Cisco Express Forwarding (CEF) on the MWR 1941-DC. Commands such as **no ip cef** will display an error message "%Cannot disable CEF on this platform." Some commands, such as **no ip route-cache cef**, will not return an error message. However, CEF will **not** be disabled regardless of whether an error message is displayed.
- If you are using the MWR 1941-DC in a redundant configuration and are attaching the MWR 1941-DC to a device that uses spanning tree, configure portfast on the device to avoid problems with HSRP at start up.
- In case of a tie in priority, HSRP uses the IP address to determine the active router. Therefore, you should ensure that the order of the IP addresses of the E1/T1 interfaces of the active router corresponds to the order of the IP addresses of the E1/T1 interfaces of the standby router.

Slot and Port Numbering

The Cisco MWR 1941-DC router chassis contains the following LAN and WAN interface types:

- Two built-in Fast Ethernet LAN interfaces
- Three slots in which you can install Voice/WAN interface cards (VWICs)
- One slot in which you can install a network module

The slot numbers are as follows:

- 0 for all built-in interfaces
- 0 for all built-in VWIC slots
- 1 for the network module slot

The numbering format is:

```
Interface type Slot number/Interface number
```

Interface (port) numbers begin at 0 for each interface type, and continue from right to left.

- The two built-in Ethernet 10/100 interfaces are Fast Ethernet 0/0 and Fast Ethernet 0/1.
- The slot number for all VWIC interfaces in the built-in VWIC slot is always 0. (The W0, W1, and W2 slot designations are for physical slot identification only.) Interfaces in the VWICs are numbered from right to left, starting with 0/0 for each interface type, regardless of the physical VWIC slot in which the VWICs are installed.

  For example, if you have a VWIC in two of the VWIC slots (W0 and W1), then the interfaces are:

  - Serial 0/0 and Serial 0/1 in physical slot W0
  - Serial 0/2 and Serial 0/3 in physical slot W1

  However, if you install a VWIC in physical slot W1 (leaving slot W0 empty), the interfaces in slot W1 are Serial 0/0 and Serial 0/1. If you then add a VWIC to slot W0, the interface numbering will shift. The configuration that you created for interfaces Serial 0/0 and Serial 0/1 will now be applied to the VWIC in slot W0 and you will need to create a new configuration for the interfaces that you previously configured on W1 (which will now be Serial 0/2 and Serial 0/3).
- The slot number of WIC/VWIC interfaces installed in slot 1 using a WAN network module is always 1 and the interfaces are always numbered from the right to left.
- The slot number for all network module interfaces is always 1 and the interfaces are always numbered from right to left starting with 1/0.

Verifying the Version of Cisco IOS Software

To implement the MWR 1941-DC router in an IP-RAN, Cisco IOS Release 12.2(8)MC2 or a later must be installed on the router. To verify the version of Cisco IOS software, use the **show version** command.

The **show version** command displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

Configuring the Host Name and Password

One of the first configuration tasks you might want to do is configure the host name and set an encrypted password. Configuring a host name allows you to distinguish multiple Cisco routers from each other. Setting an encrypted password allows you to prevent unauthorized configuration changes.

	Command	Purpose

Step 1	`Router>` **`enable`**
	`Password:` *`password`*
	`Router#`
		Enter enable mode. Enter the password.
		You have entered enable mode when the prompt changes to `Router#`.

Step 2	`Router#` **`configure terminal`**
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Router(config)#`
		Enter global configuration mode. You have entered global configuration mode when the prompt changes to `Router(config)#`.

Step 3	`Router(config)#` **`hostname Router`**
	`Router(config)#`
		Change the name of the router to a meaningful name. Substitute your host name for `Router`.

Step 4	`Router(config)#` **`enable secret guessme`**	Enter an enable secret password. This password provides access to privileged EXEC mode. When a user types **enable** at the EXEC prompt (`Router>`), they must enter the enable secret password to gain access to configuration mode. Substitute your enable secret for `guessme`.
Step 5	`Router(config)#` **`line con 0`**	Enter line configuration mode to configure the console port. When you enter line configuration mode, the prompt changes to `Router(config-line)#`.
	`Router(config-line)#` **`exec-timeout 0 0`**	Prevent the router's EXEC facility from timing out if you do not type any information on the console screen for an extended period.

	`Router(config-line)#` **`exit`**
	`Router(config)#`
		Exit back to global configuration mode.

To verify that you configured the correct host name and password:

Step 1 Enter the **show config** command:

```
Router(config)# show config
Using 1888 out of 126968 bytes
!
version XX.X
.
.
.
!
hostname Router
!
enable secret 5 $1$60L4$X2JYOwoDc0.kqa1loO/w8/
.
.
.
```

Check the host name and encrypted password displayed near the top of the command output.

Step 2 Exit global configuration mode and attempt to re-enter it using the new enable password:

```
Router# exit
.
.
.
Router con0 is now available
Press RETURN to get started.
Router> enable
Password: guessme
Router#
```

Configuring Loopback Interfaces

The loopback interface is a software-only, virtual interface that emulates an interface that is always up. The interface-number is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.

The multilink interface is a virtual interface, if you are **not** going to assign an explicit IP address to the interface, you should create a loopback interface for the multilink interface to enable IP processing on the interface.

In the case where the MWR 1941-DC is used in a redundant configuration, you must also configure loopback interfaces for the health and revertive interfaces. The health interface monitors the status of the redundant configuration so that the standby router can take over if there is a problem with the active router. The revertive interface is required to ensure that the switchover takes place. We recommend that you use 101 for the health interface and 102 for the revertive interface.

To configure a loopback interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface loopback number`	Creates a loopback interface for the multilink interface. **Note** For the health and revertive interfaces, you do not need to assign an IP address.
Step 2	`Router(config-if)# ip address ip-address subnet-mask`	Assigns an IP address and subnet mask to the interface.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.

Configuring Fast Ethernet Interfaces

To configure the FE interface of the MWR 1941-DC, complete the following tasks:

- Configuring the FE Interface IP Address
- Setting the Speed and Duplex Mode
- Configuring Routing Protocol Attributes
- Configuring PIM
- Configuring HSRP Support
- Enabling the FE Interface

Configuring the FE Interface IP Address

To configure the FE interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface fastethernet slot/port`	Specifies the port adapter type and the location of the interface to be configured. The *slot* is always 0 and the *port* is the number of the port (0 or 1).
Step 2	`Router(config-if)# ip address ip-address subnet-mask`	Assigns an IP address and subnet mask to the interface.
Step 3	`Router(config-if)# exit`	Exits interface configuration mode.

Setting the Speed and Duplex Mode

The Fast Ethernet ports of the MWR 1941-DC can run in full or half duplex mode and at 100 Mbps or 10 Mbps. The MWR 1941-DC also has an auto-negotiation feature that allows the router to negotiate the speed and duplex mode with the corresponding interface on the other end of the connection.

Auto negotiation is the default setting for the speed and transmission mode.

When configuring an interface speed and duplex mode, note these guidelines:

- If both ends of the line support auto negotiation, we highly recommend the default auto negotiation settings.
- When the auto negotiation is turned on for either speed or duplex, it auto negotiates both speed and duplex.
- If one interface supports auto negotiation and the other end does not, configure duplex and speed on both interfaces; do not use the auto setting on the supported side or the duplex setting will be half.

To configure the speed and duplex operation, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# duplex [auto	half	full]`	Specifies the duplex operation.
Step 2	`Router(config-if)# speed [auto	100	10]`	Specifies the speed.

Configuring Routing Protocol Attributes

When used in the CDMA IP-RAN solution, the MWR 1941-DC must be configured to support the OSPF routing protocol.

To configure OSPF routing protocol attributes, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# ip ospf message-digest-key key-id md5 key`	Enables OSPF Message Digest 5 (MD5) authentication.
Step 2	`Router(config-if)# ip ospf hello-interval seconds`	Configures the interval between hello packets that the Cisco IOS software sends on the interface.
Step 3	`Router(config-if)# ip ospf dead-interval seconds`	Configures the interval at which hello packets must not be seen before neighbors declare the router down.

Configuring PIM

Because the MWR 1941-DC is used in a multicast PPP environment, you should configure the Protocol Independent Multicast (PIM) mode of the FE interface.

To configure the PIM mode, use the following command while in interface configuration mode:

Command	Purpose
`Router(config-if)# ip pim {sparse-mode | sparse-dense-mode | dense-mode [proxy-register {list access-list | route-map map-name}]}`	Configures PIM on an interface, where: • **sparse-mode**—Enables sparse mode of operation. • **sparse-dense-mode**—Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in. • **dense-mode**—Enables dense mode of operation. • **proxy-register**—(Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR. • **list** *access-list*—(Optional) Defines the extended access list number or name. • **route-map** *map-name*—(Optional) Defines the route map.

Configuring HSRP Support

In redundant configurations, the MWR 1941-DC uses Cisco IOS Hot Switch Routing Protocol (HSRP) to control the active and standby routers. To use HSRP, you must configure the standby priority attributes and the IP address of the virtual router. Priority is determined first by the configured priority value, and then by the IP address. In each case a higher value is of greater priority.

Note If you do not plan to use the MWR 1941-DC in a redundant configuration, do not configure HSRP support and see Configuring Redundancy, page 28 for information about using the router in a standalone environment.

To configure HRSP, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# **standby** group **name** *group-name*	Specifies the name of the standby group. **Note** The standby group names must be "one" and "two." For FE 0/0, the command must be **standby 1 name one**. For FE 0/1, the command must be **standby 2 name two**. **Tip** If you omit the *group-name* or if you enter a group name that doesn't begin with one or two, the configuration will fail and there will be a mismatch in the information displayed by the **show redundancy** and **show standby** commands.
Step 2	Router(config-if)# **standby** *group* **ip** *address*	Enables HSRP and assigns an IP address to the virtual router. This address is the same for both the active and standby routers.
Step 3	Router(config-if)# **standby** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*	Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down. **Note** You ***must*** use 1 for the hello time and 3 for the hold time.
Step 4	Router(config-if)# **standby** *group* **preempt**	Indicates that the router can become the active router when its priority is higher than all other HSRP-configured routers. Without preemption, a standby router will only transition to the active state if HSRP "hello messages" cease. In the CDMA IP-RAN solution, there may be situations in which you want a switchover to occur in the absence of a router or FE failure, therefore, preemption is required.

	Command	Purpose
Step 5	Router(config-if)# **standby** *group* **track multilink** *number decrement-value* Router(config-if)# **standby** *group* **track loopback** *number decrement-value* Router(config-if)# **standby** *group* **track fastethernet** *number decrement-value*	Specifies other interfaces on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group. When using the MWR 1941-DC router in the CDMA IP-RAN solution, you must configure each FE interface to track the multilink interface, the loopback interfaces, and the **other** FE interface. **Note** In redundant configurations, you should issue **standby track** commands for both the health interface (loopback101) and the revertive interface (loopback102) as well as for the backhaul interface (multilink1). The decrement values ***must*** be as follows: 10 for the multilink, FE, and health interfaces; 5 for the revertive interface.
Step 6	Router(config-if)# **standby** *group* **priority 100**	Configures HSRP priority. **Note** We recommend that you specify a priority of 100.

Note If you are using the MWR 1941-DC in a redundant configuration, you must also set the keepalives under the FE interface to 1.

```
Router(config-if)# keepalive 1
```

Enabling the FE Interface

Once you have configured the FE interface, you can enable it.

To enable the FE interface, use the following command while in interface configuration mode:

Command	Purpose
Router(config-if)# **no shutdown**	Enables the interface.

Configuring Multilink Interfaces

To configure the multilink interfaces, complete the following tasks:

- Configuring Multilink PPP, page 17
- Configuring IP Address Assignment, page 18
- Configuring PPP Multiplexing, page 18
- Configuring RTP/UDP Compression, page 20
- Configuring the RTP/UDP Compression Flow Expiration Timeout Duration, page 21
- Configuring Routing Protocol Attributes, page 22
- Configuring PIM, page 22

Configuring Multilink PPP

As higher-speed services are deployed, Multilink-PPP (MLP) provides a standardized method for spreading traffic across multiple WAN links, while providing multivendor interoperability and load-balancing on both inbound and outbound traffic.

A Multilink interface is a special virtual interface which represents a multilink PPP bundle. The multilink interface serves to coordinate the configuration of the bundled link, and presents a single object for the aggregate links. However, the individual PPP links that are aggregated together, must also be configured. Therefore, to enable Multilink PPP on multiple serial interfaces, you need to first set up the multilink interface, and then configure each of the serial interfaces and add them to the same multilink interface.

The MWR 1941-DC router can support up to 16 T1 interfaces through the multilink interface.

To set up the multilink interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`RPM(config)#` **`interface multilink`** *`number`*	Specifies the multilink interface to be configured.
Step 2	`RPM(config-if)#` **`ppp multilink`**	Enables multilink PPP operation.
Step 3	`RPM(config-if)#` **`multilink-group`** *`group-number`*[1] or `RPM(config-if)#` **`ppp multilink group`** *`group-number`*[2]	Specifies an identification number for the multilink interface.
Step 4	`RPM(config-if)#` **`ip unnumbered loopback`** `number`	Enables IP processing on the multilink interface without assigning an explicit IP address to the interface, where *number* is the number of the loopback interface that you configured in Configuring Multilink PPP.

[1] Cisco IOS Release 12.2(15)MC2a or later.

[2] Cisco IOS 12.3(11)T or later.

Configuring IP Address Assignment

A point-to-point interface must be able to provide a remote node with its IP address through the IP Control Protocol (IPCP) address negotiation process. The IP address can be obtained from a variety of sources. The address can be configured through the command line, entered with an EXEC-level command, provided by TACACS+ or the Dynamic Host Configuration Protocol (DHCP), or from a locally administered pool.

IP address pooling uses a pool of IP addresses from which an incoming interface can provide an IP address to a remote node through IPCP address negotiation process. IP address pooling also enhances configuration flexibility by allowing multiple types of pooling to be active simultaneously.

To configure IP address assignment, use the following command while in multilink interface configuration mode:

Command	Purpose
`RPM(config-if)#` **`peer default ip address`** `{`*`ip-address`* `|` **`dhcp`** `|` **`pool`** `[`*`pool-name`*`]}`	Specifies an IP address, an address from a specific IP address pool, or an address from the Dynamic Host Configuration Protocol (DHCP) mechanism to be returned to a remote peer connecting to this interface.

Configuring PPP Multiplexing

To enable and control the multiplexing of PPP frames, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#` **`ppp mux`**	Enables PPP multiplexing.
Step 2	`RPM(config-if)#` **`ppp mux delay`** *`integer`*	Sets the maximum time delay.
Step 3	`RPM(config-if)#` **`ppp mux subframe length`** *`integer`*	Sets the maximum length of the subframe.
Step 4	`RPM(config-if)#` **`ppp mux frame`** *`integer`*	Sets the maximum length of the superframe
Step 5	`RPM(config-if)#` **`ppp mux subframe count`** *`integer`*	Sets the maximum number of subframes in a superframe.
Step 6	`RPM(config-if)#` **`ppp mux pid`** *`integer`*	Sets the default PPP protocol ID.

Configuring ACFC and PFC Handling During PPP Negotiation

With Cisco IOS Release 12.2(15)MC1 and later, ACFC and PFC handling during PPP negotiation can be configured. By default, ACFC/PFC handling is not enabled.

To configure ACFC handling during PPP negotiation, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#  ppp acfc remote {apply | reject | ignore}`	Configures how the router handles the ACFC option in configuration requests received from a remote peer, where: • **apply**—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer. • **reject**—ACFC options are explicitly ignored. • **ignore**—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.
Step 2	`RPM(config-if)# ppp acfc local {request | forbid}`	Configures how the router handles ACFC in its outbound configuration requests, where: • **request**—The ACFC option is included in outbound configuration requests. • **forbid**—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.

To configure PFC handling during PPP negotiation, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)# ppp pfc remote {apply	reject	ignore}`	Configures how the router handles the PFC option in configuration requests received from a remote peer, where: • **apply**—PFC options are accepted and PFC may be performed on frames sent to the remote peer. • **reject**—PFC options are explicitly ignored. • **ignore**—PFC options are accepted, but PFC is not performed on frames sent to the remote peer.
Step 2	`RPM(config-if)# ppp pfc local {request	forbid}`	Configures how the router handles PFC in its outbound configuration requests, where: • **request**—The PFC option is included in outbound configuration requests. • **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.

Configuring RTP/UDP Compression

Enabling RTP/UDP compression (cRTP/cUDP) on both ends of a low-bandwidth serial link can greatly reduce the network overhead if there is a lot of RTP traffic on that slow link. This compression is beneficial especially when the RTP payload size is small (for example, compressed audio payloads of 20-50 bytes).

Note Before you can enable RTP header compression, you must configure a serial line that uses PPP encapsulation.

To configure RTP header compression when using Cisco IOS Release 12.2(15)MC2a or prior, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)# ip rtp header-compression`	Enables RTP header compression for serial encapsulations.
Step 2	`RPM(config-if)# ip rtp compression-connections` *`number`*	Configures the total number of RTP header compression connections on an interface. By default, a total of 16 RTP compression connections on an interface is supported.

To configure RTP header compression when using Cisco IOS Release 12.3(11)T or later, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)# ip rtp header-compression ignore-id`	Enables RTP header compression for serial encapsulations and suppresses IP ID checking during RTP compression.
Step 2	`RPM(config-if)# ip rtp compression-connections number`	Configures the total number of RTP header compression connections on an interface. By default, a total of 16 RTP compression connections on an interface is supported.

Note The MWR 1941-DC supports up to 1000 RTP header compression connections on an interface.

Configuring the RTP/UDP Compression Flow Expiration Timeout Duration

To minimize traffic corruption, cUDP flows expire after a period of time during which no packets are passed. When this user defined duration of inactivity occurs on a flow at the compressor, the compressor sends a full header upon receiving a packet for that flow, or, if no new packet is received for that flow, the compressor makes the CID for the flow available for new use. When a packet is received at the decompressor after the duration of inactivity has been exceeded, the packet is dropped and a context state message is sent to the compressor requesting a flow refresh.

The default expiration timeout is 5 seconds. The recommended value is 8 seconds.

Caution Failure of performance/latency scripts could occur if the expiration timeout duration is not changed to the recommended 8 seconds.

To configure the duration of the cUDP flow expiration timeout, use the following command while in multilink interface configuration mode:

Command	Purpose
`RPM(config-if)# ppp iphc max-time seconds`	Specifies the duration of inactivity, in seconds, that when exceeded causes the cUDP flow to expire.

Configuring Routing Protocol Attributes

When used in the CDMA IP-RAN solution, the multilink interface must be configured to support the OSPF routing protocol.

To configure OSPF routing protocol attributes, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)# ip ospf message-digest-key key-id md5 key`	Enables OSPF Message Digest 5 (MD5) authentication.
Step 2	`RPM(config-if)# ip ospf hello-interval seconds`	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
Step 3	`RPM(config-if)# ip ospf dead-interval seconds`	Sets the interval at which hello packets must not be seen before neighbors declare the router down.

Configuring PIM

Because the MWR 1941-DC is used in a multicast PPP environment, you should configure the PIM mode of the multilink interface.

To configure the PIM mode, use the following command while in interface configuration mode:

Command	Purpose
`RPM(config-if)# ip pim {sparse-mode | sparse-dense-mode | dense-mode [proxy-register {list access-list | route-map map-name}]}`	Configures PIM on an interface, where: • **sparse-mode**—Enables sparse mode of operation. • **sparse-dense-mode**—Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in. • **dense-mode**—Enables dense mode of operation. • **proxy-register**—(Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR. • **list** *access-list*—(Optional) Defines the extended access list number or name. • **route-map** *map-name*—(Optional) Defines the route map.

Configuring T1 and E1 Interfaces

To configure a T1/E1 multiflex trunk interface, enter the following Cisco IOS commands at the router prompt.

Note Before you begin, disconnect all WAN cables from the router to keep it from trying to run the AutoInstall process. The router tries to run AutoInstall whenever you power it on if there is a WAN connection on both ends and the router does not have a valid configuration file stored in NVRAM (for instance, when you add a new interface). It can take several minutes for the router to determine that AutoInstall is not connected to a remote Transmission Control Protocol/Internet Protocol (TCP/IP) host.

Configuring T1 Interfaces

To configure the T1 interfaces, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# controller t1 slot/port`	Specifies the controller that you want to configure. For information about interface numbering, see "Slot and Port Numbering" section on page 9.
Step 2	`Router(config-controller)# framing esf`	Specifies the framing type.
Step 3	`Router(config-controller)# linecode b8zs`	Specifies the line code format.
Step 4	`Router(config-controller)# channel-group 0 timeslots 1-24 speed 64`	Specifies the channel group and time slots to be mapped. For the VWIC interfaces, you can configure two channel-groups (0 and 1) on the first T1 port or you can configure one channel-group (0 or 1) on each T1 port. Once you configure a channel group, the serial interface is automatically created. **Note** The default speed of the channel group is 56. To get full DS0/DS1 bandwidth, you must configure a speed of 64.
Step 5	`Router(config-controller)# cablelength feet`	Configures the cable length. **Note** Although you can specify a cable length from 0 to 450 feet, the hardware only recognizes two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.
Step 6	`Router(config-controller)# exit`	Exits controller configuration mode.
Step 7	`Router(config)# interface serial slot/port:0`	Configures the serial interface. Specify the T1 slot (always 0), port number, and channel group.

	Command	Purpose
Step 8	`Router(config-if)#` **`ip address`** *`ip-address subnet-mask`*	Assigns an IP address and subnet mask to the interface. If the interface is a member of a Multilink bundle (MLPPP), then skip this step.
Step 9	`Router(config-if)#` **`encapsulation ppp`**	Configures PPP encapsulation. **Note** Before you can enable RTP header compression, you must have configured a serial line that uses PPP encapsulation.
Step 10	`Router(config-if)#` **`keepalive`** `[`*`period`* `[`*`retries`*`]]`	Enables keepalive packets on the interface and specify the number of times keepalive packets will be sent without a response before bringing down the interface. **Note** When enabled in an IP-RAN solution, the recommended configuration is **keepalive 1 2** on both the MWR 1941-DC serial interface and associated MGX-RPM-1FE-CP virtual template interface.
Step 11	`Router(config-if)#` **`carrier-delay`** *`number`*	Sets the carrier delay for the serial interface.
Step 12	`Router(config-if)#` **`exit`**	Exits to global configuration mode.

Return to Step 1 to configure the second port on the VWIC and the ports on any additional VWICs.

Configuring E1 Interfaces

To configure the E1 interfaces, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`controller e1`** *`slot`*`/`*`port`*	Specifies the controller that you want to configure. Controller E1 0/0 maps to the first port of the VWIC in slot 0. Controller E1 0/1 maps to the second port of the VWIC in slot 0.
Step 2	`Router(config-controller)#` **`framing crc4`**	Specifies the framing type.
Step 3	`Router(config-controller)#` **`linecode hdb3`**	Specifies the line code format.
Step 4	`Router(config-controller)#` **`channel-group 0 timeslots 1-24 speed 64`**	Specifies the channel group and time slots to be mapped. For the VWIC interfaces, you can configure channel-group 0 and 1 on one port or one channel-group (either 0 or 1) on each port. Once you configure a channel group, the serial interface is automatically created. **Note** The default speed of the channel group is 56. To get full DS0/DS1 bandwidth, you must configure a speed of 64.

	Command	Purpose
Step 5	`Router(config-controller)# interface serial slot/port:0`	Configures the serial interface. Specify the E1 slot (always 0), port number, and channel group.
Step 6	`Router(config-controller)# cablelength feet`	Configures the cable length. **Note** Although you can specify a cable length from 0 to 450 feet, the hardware only recognizes two ranges: 0 to 49 and 50 to 450. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no change because 40 is within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range is used. The actual number you enter is stored in the configuration file.
Step 7	`Router(config-if)# ip address ip-address subnet-mask`	Assigns an IP address and subnet mask to the interface. If the interface is a member of a Multilink bundle (MLPPP), then skip this step.
Step 8	`Router(config-if)# encapsulation ppp`	Configures PPP encapsulation. Before you can enable RTP header compression, you must have configured a serial line that uses PPP encapsulation
Step 9	`Router(config-if)# keepalive [period [retries]]`	Enables keepalive packets on the interface and specify the number of times keepalive packets will be sent without a response before bringing down the interface. **Note** When enabled in an IP-RAN solution, the recommended configuration is **keepalive 1 2** on both the MWR 1941-DC serial interface and associated MGX-RPM-1FE-CP virtual template interface.
Step 10	`Router(config-if)# carrier-delay number`	Sets the carrier delay for the serial interface.
Step 11	`Router(config-if)# exit`	Exits to global configuration mode.

Return to Step 1 to configure the second port on the VWIC and the ports on any additional VWICs.

Configuring QoS Attributes

To use QoS on the MWR 1941-DC router, you must first create a class map. The class map defines the criteria that a packet must match to be placed in that class. Once you have created a class map, the router can recognize packets that are subject to QoS. You must then tell the router the action to take on those packets by creating a policy map.Once you have completed the creation of a QoS boilerplate, you can assign it to an interface.

Note The QoS functionality of the MWR 1941-DC router is built on the same code as the Cisco 10000 ESR (with some exceptions). For more information about the QoS feature, see *Configuring Quality of Service* (http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10ksw/qosos.htm) and the *Cisco 10000 Series ESR Quality of Service* feature module (http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10kfm/fm_qos.htm), as well as the *Cisco IOS Quality of Service Solutions Configuration Guide* and the *Cisco IOS Quality of Service Solutions Command Reference*.

Creating a Class Map

For each class map that you want to create, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **class-map** [**match-all** | **match-any**] *class-name*	Assigns a name to your class map, where: • **match-any** means a single match rule is sufficient for class membership • **match-all** means only those packets that have all the attributes you specify are part of the class When you enter the **class-map** command, you are placed in class map configuration mode.
Step 2	Router(config-cmap)# **match access-group** *number* Router(config-cmap)# **match ip dscp** *number* Router(config-cmap)# **match ip precedence** *number* Router(config-cmap)# **match input-interface** *interface-name* Router(config-cmap)# **match protocol** *protocol*	Describes the characteristics of the packets that are subject to QoS (can use one or more): • **match access-group** specifies access control list (ACL) that a packet must match. • **match ip dscp** specifies the IP differentiated service code point (DSCP) that a packet must match. • **match ip precedence** specifies the precedence values (0-7) that a packet must match. • **match input-interface** specifies the name of the input interface used as a match criterion. • **match input-protocol** specifies the protocol that a packet must match. **Note** For more information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference*.
Step 3	Router(config-cmap)# **exit**	Exits class map configuration mode.

Creating a Policy Map

To create a policy map, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **policy-map** *policy-name*	Assigns a name to your policy map. When you enter the **policy-map** command, you are placed in policy map configuration mode.
Step 2	Router(config-pmap)# **class** *class-name*	Associates the policy map with a class map. Specify the same *class-name* as you did in Step 1 of the "Creating a Class Map" section on page 26. When you enter the **class** command, you are placed in class submode of the policy-map configuration mode.
Step 3	Router(config-pmap-c)# **priority percent** *number* Router(config-pmap-c)# **bandwidth percent** *number* Router(config-pmap-c)# **queue-limit** *number* Router(config-pmap-c)# **priority** *rate-in-kbps* Router(config-pmap-c)# **shape** {**average** | **peak**} *cir* [*bc*] [*be*] Router(config-pmap-c)# **shape max-buffers** *number-of-buffers*	Describes the QoS actions you want the router to perform when the router encounters a packet that has the characteristics described by the class map (use one or more commands): • **priority percent** gives priority to a class of traffic belonging to a policy map and specifies that a certain percentage of the available bandwidth should be reserved for this class. • **bandwidth percent** specifies the bandwidth allocated for a class belonging to a policy map. • **queue-limit** specifies the maximum number of packets the queue can hold for a class policy configured in a policy map. • **priority** enables low-latency priority queuing, which allows you to assign a specified share of the link bandwidth to one queue that receives priority over all others. Low-latency priority queueing minimizes the packet-delay variance for delay-sensitive traffic, such as live voice and video. • **shape** and **shape max-buffers** are used with class-based weighted fair queuing (CB-WFQ), which allows you to control the traffic going out an interface in order to match its transmission to the speed of the remote target interface. **Note** The **bandwidth percent** and **priority percent** commands cannot be used in the same class, within the same policy map. These commands can be used together in the same policy map, however. For more information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference.*

	Command	Purpose

Step 4	`Router(config-pmap-c)# set ip dscp ip-dscp-value`
	`Router(config-pmap-c)# set ip precedence ip-precedence-value`
	`Router(config-pmap-c)# set qos-group qos-group-value`
		Configures the Class-Based Packet Marking feature, you must configure either an IP Precedence value or an IP differentiated services code point (DSCP). The QOS group is optional.
		• **set ip dscp** marks a packet by setting the IP DSCP value.
		• **set ip precedence** marks a packet by setting the IP Precedence bits in the ToS byte.
		• **set qos-group** associates a local QoS group value with a packet.
		For more information about these commands, see the "*Cisco IOS Quality of Service Solutions Command Reference*."

Step 5	`Router(config-pmap-c)# exit`	Exits the class submode of the policy map configuration mode. Repeat Step 2 and Step 3 for each class map.
Step 6	`Router(config-pmap)# exit`	Exits to global configuration mode.

Assigning a QoS Boilerplate to an Interface

To assign a QoS boilerplate to a multilink interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface multilink number`	Accesses the multilink interface configuration mode.
Step 2	`Router(config-if)# service-policy output policy-name`	Assigns the QoS boilerplate to the multilink interface.

Configuring Redundancy

The MWR 1941-DC router can be used in either a redundant configuration (preferable) or as a standalone device.

Note Before implementing redundancy, you must disable EADI capabilities on the router using the **diable-eadi** global configuration command and also configure HSRP under the Fast Ethernet interface. See the "Configuring HSRP Support" section on page 14 for more information on configuring HSRP under the Fast Ethernet interface.

Redundant MWR 1941-DCs

For redundancy, the MWR 1941-DC router makes use of the existing HSRP feature. However, additional controls are needed for the MWR 1941-DC. In a redundant configuration, the MWR 1941-DC router must track the status of the health and revertive loopback interfaces as well as the backhaul interface.

To configure an MWR 1941-DC for use in a redundant configuration, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **redundancy**	Enters redundancy mode.
Step 2	Router(config-r)# **mode y-cable**	Enters the y-cable mode.
Step 3	Router(config-r-y)# **standby use-interface** *interface* **health** Router(config-r-y)# **standby use-interface** *interface* **revertive**	Specifies the loopback interface to be used to monitor the health of the router and for revertive purposes. **Note** The interfaces that you specify for the health and revertive interfaces should match those that you configured and tracked in Configuring Loopback Interfaces. (We recommend you use loopback101 for the health and loopback102 for the revertive interface).
Step 4	Router(config-r-y)# **standby use-interface** *interface* **backhaul**	Specifies the interface to be used for backhauling. **Note** 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. The interface that you specify for the backhaul interface should match one of those that you configured and tracked in Configuring Loopback Interfaces.
Step 5	Router(config-r-y)# **exit**	Exits y-cable configuration mode.

To verify the status of the relays on an MWR 1941-DC router, use the **show controllers** command.

Standalone MWR 1941-DC

The MWR 1941-DC router has relays that work with a special “y” cable for redundancy and are controlled by HSRP. You can, however, use the MWR 1941-DC as a standalone device. If you choose not to use the MWR 1941-DC in a redundant configuration, you should **not** configure HSRP and you must control the relays of the VWIC card manually.

To manually set the relays to open or closed, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# `**`redundancy`**	Enters redundancy mode.
Step 2	`Router(config-r)# `**`mode y-cable`**	Enters the y-cable mode.
Step 3	`Router(config-r-y)# `**`standalone`**	Specifies that the router is to be used as a stand-alone device. This command closes the relays.
Step 4	`Router(config-r-y)# `**`exit`**	Exits y-cable configure mode.

To verify the status of the relays on an MWR 1941-DC router, use the **show controllers** command.

Configuring the Link Noise Monitor

Note This feature requires Cisco IOS Release 12.2(8)MC2d and later be installed on the MWR 1941-DC router.

Noise on T1 and E1 links that span between the BTS and central office can affect voice quality for mobile users to the point where it becomes unacceptable. To monitor the quality of individual links in a multilink bundle, you can configure the Link Noise Monitor (LNM) on your MWR 1941-DC router

The LNM detects, alerts, and removes noisy links from a bundle based on user-defined thresholds and durations. In addition, the LNM notifies the operator once the quality of the line has improved, and restores the link service if the link has been removed.

Specifically, to detect noise on a link, the LNM monitors the following two types of errors which make up the Bit Error Rate (BER) and compares the number of errors with the user-defined thresholds:

- Line Code Violation (LCV)—A Bi-Polar Violation (BPV) or Excessive Zeroes (EXZ) error has occurred.
- Path Code Violation (PCV)—A Cyclic Redundancy Check (CRC) error, which is generally caused by one or more LCV or logic errors, has occurred in a time slot.

The LNM provides the following types of noise monitors:

- Link Warning—Issues a warning when the noise level of a link exceeds a user-defined threshold and notifies the operator when the noise level improves to the point that it drops below a second user-defined threshold.
- Link Removal—Issues an error and removes a link from service when the noise level of the link exceeds a user-defined threshold and restores the link and provides notification when the noise level improves to the point that it drops below a second user-defined threshold.

Note If the noise level on the last active link in a multilink bundle exceeds the Link Removal threshold, an alert is issued but the link will not be removed from service. If this situation occurs, the standard T1 error rate is used to determine if the last active link must be removed from service.

Usage Notes

When configuring the LNM, please note the following:

- If the **warn** and **remove** keywords are specified without any other options, the LCV and PCV thresholds and duration defaults will be use to determine (**set**) and clear (**clear**) the condition.
- If the **span** command is issued with the **set** keyword specified (defining the LNM type and parameters to use to determine a condition exists) and the command is not issued again with the **clear** keyword specified (defining the parameters used to clear a condition), or vice versa, the values configured for the threshold and duration will be used for both.
- If the **span** command is issued without either the **set** or **clear** keywords specified, **set** is the default.
- The **set** and **clear** keywords can only be specified if the threshold or duration has been specified.
- If the PCV threshold is not configured (using the **pcv** keyword and value), the threshold is calculated using Gaussian probability distribution that is representative of most noise environments.
- The following SYSLOG messages have been added for fault notification:

```
- %LNM-4- WARNEXCEED:Controller <Controller IF>, exceeded noise warning threshold
  <int>, duration <int>
- %LNM-4- WARNIMPROVE:Controller <Controller IF>, noise improved below threshold
  <int>, duration <int>
- %LNM-2-REMOVE:Interface <Serial IF> removed, noise exceeded threshold <int>,
  duration <int>
- %LNM-2- RESTORE:Interface <Serial IF> restored, noise improved below threshold
  <int>, duration <int>
- %LNM-2- REMEXCEED:Interface <Serial IF>, noise exceeded threshold <int>,
  duration <int>
- %LNM-2- REMIMPROVE:Interface <Serial IF>, noise improved below threshold <int>,
  duration <int>
```

Configuring LNM

To configure the LNM feature, issue the **span** command from controller configuration mode of each T1 or E1 link in the bundle that you want to monitor. To disable LNM on a link, issue the **no** version of the command from controller configuration mode of the link.

span {**warn** | **remove**} [{[**lcv** *value* [**pcv** *value*]] [**duration** *seconds*]} **set** | **clear**]

where:

- **warn**—Enables Link Warning monitoring on the link.
- **remove**—Enables Link Removal monitoring on the link.
- **lcv** *value*—Threshold (in bit errors per second) that when exceeded for the configured duration when the **set** keyword has been specified, creates a condition (warning or link removal), or when fallen below for the configured duration when the **clear** keyword has been specified, clears the condition.

  For T1 links:

  - Valid range is 5 to 1544.
  - For Link Warning monitoring, the default is 15.
  - For Link Removal monitoring, the default is 154.

  For E1 links,

  - Valid range is 7 to 2048.
  - For Link Warning monitoring, the default is 20.
  - For Link Removal monitoring, the default is 205.
- **pcv** *value*—Number of time slots in errors per second. If not specified by the user, this value is calculated from the LCV threshold based on a Gaussian distribution that matches typical noise-induced errors.

  For T1 links:

  - Valid range is 3 to 320.
  - For Link Warning monitoring, the default is 15.
  - For Link Removal monitoring, the default is 145.

  For E1 links,

  - Valid range is 8 to 832.
  - For Link Warning monitoring, the default is 20.
  - For Link Removal monitoring, the default is 205.
- **duration** *seconds*—Number of seconds that a threshold must be exceeded to create a condition or fallen below to clear a condition. Valid range is 1 to 600. The default is 10.

  When specified with th**e lcv** keyword, the duration must be configured after the LCV threshold. For example, **span warn lcv 55 duration 20** is a correct way to issue the command; s**pan warn duration 20 lcv 55** is not.
- **set**—Specifies that the values configured for the **span** command are to be used to set a condition.
- **clear**—Specifies that the values configured for the **span** command are to be used to clear a condition.

Saving the Configuration

To prevent the loss of the router configuration, save it to non-volatile random access memory (NVRAM). To save the configuration to NVRAM, use the following command while in global configuration mode:

Command	Purpose
`Router# copy running-config startup-config`	Saves the configuration changes to NVRAM so that they are not lost during resets, power cycles, or power outages.

Verifying the Configuration

To verify the configuration of the MWR 1941-DC, enter the following command:

```
Router# show running-config

hostname MWR1900-1
!
boot system slot0:mwr-1900-boot
!
! description Loopback IP for O & M
!
interface loopback 0
 ip address 10.1.170.3 255.255.255.255
!
! description Loopback IP for IP Unnumbered
!
interface loopback 2
 ip address 192.168.170.2 255.255.255.255
!
interface loopback101
 description Health Loopback Interface
 no ip address
!
interface loopback102
 description Revertive Loopback Interface
 no ip address
!
enable password cisco
!
memory-size iomem 25
!
redundancy
  mode y-cable
   standby use-interface Loopback101 health
   standby use-interface Loopback102 revertive
   standby use-interface Multilink2 backhaul
!
controller T1 0/0
 framing esf
 cablelength short 133ft
 clock source internal
 linecode b8zs
 channel-group 0 timeslots 1-1 speed 64
 channel-group 1 timeslots 2-24 speed 64
!
controller T1 0/1
 framing esf
 clock source internal
 linecode b8zs
 cablelength short 133ft
!
!
class-map match-all class1_fch
 match ip dscp cs5
class-map match-all class2_sch
 match ip dscp cs4
class-map match-any class3_paging_ospf
 match ip dscp cs3
match access-group 101
!
policy-map llq-policy
 class class1_fch
  priority percent 68
 class class2_sch
  bandwidth percent 20
  queue-limit 128
 class class3_paging_ospf
  bandwidth percent 2
  queue-limit 128
 class class-default
  queue-limit 512
!
ip dhcp excluded-address 192.168.146.1 192.168.146.3
ip dhcp ping packets 0
!
ip dhcp pool pbts
 network 192.168.146.0 255.255.255.0
 bootfile CENOMIbts.img
 next-server OMCR-IPaddr
 option 43 ascii "Logical-IPaddr CENOMI-IPaddr another-IPaddr SpanMapping"
 default-router 192.168.146.3
 dns-server OMCR-IPaddr
 lease 0 0 1
!
ip routing
ip subnet-zero
ip classless
ip multicast-routing
ip tftp source-interface Loopback 0
cdp run
!
! Setup sys logging to OMCIP-CW2000
!
logging on
logging buffered 4
logging cw4mw
logging trap 5
logging source-interface Loopback0
!
! Setup SNMP
!
snmp community private rw
snmp community public ro
snmp-server enable traps
snmp-server trap-source Loopback 0
snmp-server host cw4mw public
!
! Setup useful aliases
!
ip host omcr OMCR_ip_address
ip host omcip OMCIP_ip_address
ip host cw4mw CW4MW_ip_address
ip host btsha-other-0 192.168.146.2
ip host btsha-other-1 192.168.147.2
!
!interface Multilink1
description Backhaul Interface
ip unnumbered loopback 2
 cdp enable
 ppp multilink
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 ip ospf message-digest-key 1 md5 mymd5pw
!
interface Multilink2
 description
 ip unnumbered loopback 2
 ip mroute-cache
 ip mtu 256
 cdp enable
 ppp multilink
 ip rtp header-compression ignore-id
 ip rtp compression-connections 700
 ppp mux
 ppp mux subframe length 64
 ppp mux subrame count 15
 ppp mux frame 256
 ppp mux delay 800
 ppp mux pid 0x2067
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 ip ospf message-digest-key 1 md5 mymd5pw
 ip pim sparse-mode
 ip pim version 2
 service-policy output llq-policy
!
interface FastEthernet0/0
 ip address 192.168.146.1 255.255.255.0
 no ip proxy-arp
 no ip mroute-cache
 keepalive 1
 full-duplex
 speed 100
 ntp broadcast version 3
 standby 1 ip 192.168.146.3
 standby 1 timers 1 3
 standby 1 priority 100
 standby 1 preempt
 standby 1 name one
 standby 1 track FastEthernet0/1 10
 standby 1 track Loopback101 10
 standby 1 track Loopback102 5
 standby 1 track Multilink2 10
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 ip ospf message-digest-key 1 md5 mymd5pw
 ip pim sparse-mode
 ip pim version 2
 ip pim query-interval 2

interface FastEthernet0/1
 ip address 192.168.147.1 255.255.255.0
 standby 2 timers 1 3
 standby 2 preempt
 standby 2 priority 100
 standby 2 ip 192.168.147.3
 standby 2 name two
 standby 2 track Fa0/0 10
 standby 2 track Multilink2 10
 standby 2 track Loopback101 10
 standby 2 track Loopback102 5
 keepalive 1
 speed 100
 full-duplex
 ntp broadcast version 3
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 ip ospf message-digest-key 1 md5 mymd5pw
 ip pim sparse-mode
 ip pim version 2
 ip pim query-interval 2
!
!
!interface Serial0/0:0
 no ip address
 encapsulation ppp
 keepalive 1 2
 ppp multilink
 ppp multilink group 1
!
interface Serial0/1:0
 no ip address
 encapsulation ppp
 keepalive 1 2
 ppp multilink
 ppp multilink group 2
!
router ospf 1
 log-adjacency-changes
 area 2 nssa
 area 2 authentication message-digest
 auto-cost reference-bandwidth 10240
 timers spf 1 10
 redistribute ospf 2 metric-type 1 subnets
 redistribute static metric-type 1 subnets
 network 192.168.170.2 0.0.0.3 area 2
 distribute-list 10 out
 distance ospf external 125
 summary-address area-51-prefix mask
!
router ospf 2
 log-adjacency-changes
 auto-cost reference-bandwidth 10240
 area 51 authentication message-digest
 timers spf 1 10
 redistribute ospf 1 metric-type 1 subnets tag 202051
 network 192.168.146.0 0.0.0.255 area 51
 network 192.168.147.0 0.0.0.255 area 51
 network 10.0.0.0 0.255.255.255 area 51
 default-information originate metric 100 metric-type 1
 distribute-list 11 out
 distance 120
!
ip route 10.102.16.25 255.255.255.255 FastEthernet0/0
ip route 10.102.16.25 255.255.255.255 192.168.1.10
!
```

Notes

- Keepalives must be set for all Ethernet interfaces to ensure proper redundant behavior. A keepalive value of 1 has been selected for maximum responsiveness.
- Configuring **no ip proxy-arp** is helpful to avoid confusion with routes and ARP caches.
- In a redundant configuration, both MWR 1941-DCs share a common IP address for their Multilink interface.

Monitoring and Maintaining the MWR 1941-DC Router

To monitor and maintain the MWR 1941-DC router (including the multilink, VWIC, and FE interfaces) and to view information about the PPP mux and header compression configuration, use the following commands:

Command	Purpose
`Router#` **`clear counters fastethernet`** *`slot`***`/`***`port`*	Clears interface counters.
`Router#` **`clear ip rtp header-compression`**	Clears RTP header compression structures and statistics.
`Router#` **`clear ppp mux`** *`interface`*	Clears the PPP multiplexing interface counters.
`Router#` **`show controllers fastethernet`** *`slot`***`/`***`port`*	Displays information about initialization block, transmit ring, receive ring and errors for the Fast Ethernet controller chip.
`Router#` **`show controllers t1`** *`slot`***`/`***`port`*	Displays information about the cable length, framing, firmware, and errors associated with the T1. With the MWR 1941-DC, this command also displays the status of the relays on the VWIC.
`Router#` **`show ip rtp header-compression`**	Displays RTP header compression statistics.
`Router#` **`show interfaces fastethernet`** *`slot`***`/`***`port`*	Displays the status of the FE interface.
`Router#` **`show ppp multilink`**	Displays MLP and multilink bundle information.
`Router#` **`show ppp multilink interface`** *`number`*	Displays multilink information for the specified interface.
`Router#` **`show ppp mux interface`** *`interface`*	Displays statistics for PPP frames that have passed through a given multilink interface.
`Router#` **`show redundancy`**	Displays current redundant setting and recent changes in state.
`Router#` **`show standby`**	Displays HSRP configuration information.

Enabling Remote Management of the MWR 1941-DC Router

You can use Cisco's network management applications, such as CiscoWorks2000 for Mobile Wireless (CW4MW), to monitor and manage aspects of the MWR 1941-DC.

To enable remote network management of the MWR 1941-DC, do the following:

Step 1 At the privileged prompt, enter the following command to access configuration mode:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Step 2 At the configuration prompt, enter the following command to assign a host name to each of the network management workstations:

```
Router(config)# ip host hostname ip-address
```

Where *hostname* is the name assigned to the Operations and Maintenance (O&M) workstation and *ip-address* is the address of the network management workstation.

Step 3 Enter the following commands to create a loopback interface for O&M:

```
Router(config)# interface loopback number
Router(config-if)# ip address ip-address subnet-mask
```

Step 4 Exit interface configuration mode:

```
Router(config-if)# exit
```

Step 5 At the configuration prompt, enter the following command to specify the recipient of a Simple Network Management Protocol (SNMP) notification operation:

```
Router(config)# snmp-server host hostname [traps | informs] [version {1 | 2c | 3 [auth |
noauth | priv]}] community-string [udp-port port] [notification-type]
```

Where *hostname* is the name assigned to the CW4MW workstation with the **ip host** command in Step 2.

Step 6 Enter the following commands to specify the public and private SNMP community names:

```
Router(config)# snmp-server community public RO
Router(config)# snmp-server community private RW
```

Step 7 Enter the following command to enable the sending of SNMP traps:

```
Router(config)# snmp-server enable traps
```

Step 8 Enter the following command to specify the loopback interface from which SNMP traps should originate:

```
Router(config)# snmp-server trap-source loopback number
```

Where *number* is the number of the loopback interface you configured for the O&M in Step 3.

Step 9 At the configuration prompt, press Ctrl-Z to exit configuration mode.

Step 10 Write the new configuration to nonvolatile memory as follows:

```
Router# copy running-config startup-config
```

Related Documentation

This following documents contain important information about the Cisco MWR 1941-DC router:

- *Cisco MWR 1941-DC Hardware Installation Guide*
- *Cisco MWR 1941-DC Router Software Configuration Guide*
- *Regulatory Compliance and Safety Information for the Cisco MWR 1941-DC Router*
- *Cisco MWR 1941-DC Mobile Wireless Edge Router Rack Mounting Instructions*
- Cisco MWR 1941-DC Router Release Notes for Cisco IOS Release 12.x

MGX-RPM-1FE-CP Back Card with the Cisco IOS IP-RAN Feature Set

This document contains the following sections:

- Feature Overview, page 1
- Configuration Tasks, page 5
- Monitoring and Maintaining the MGX-RPM-1FE-CP Back Card, page 16
- Configuration Tasks, page 5

Feature Overview

The MGX-RPM-1FE-CP (one-port, Fast Ethernet-Co-processor) back card is an MGX8850/RPM-PR back card that off-loads the following processes from the Route Processor Module (RPM-PR):

- Compression/decompression of Real-time Transport Protocol (RTP)/User Datagram Protocol (UDP) headers (cRTP/cUDP)
- Multiplexing/demultiplexing of Point-to-Point Protocol (PPP) frames

The MGX-RPM-1FE-CP back card is designed to be used with an MGX8850 that is equipped with one or more RPM-PRs and that terminates some number of T1 lines. Each MGX-RPM-1FE-CP back card has a termination capacity of up to eight T1s (four per Multilink PPP [MLP] bundle). The MGX-RPM-1FE-CP is only supported with the MLP encapsulation.

The MGX-RPM-1FE-CP back card contains one Fast Ethernet (100Base-Tx) interface. The interface has an RJ45 connector that is used to connect the card to a Category 5 un-shielded twisted pair (UTP) cable. Both half- and full-duplex operation are supported.

PPP Multiplexing/Demultiplexing

Encapsulated PPP frames contain several bytes of header information, which adds considerable overhead to a network that is used to transport PPP frames.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

RFC 3153, PPP Multiplexing, describes a way to overcome this overhead. On the sending end, a multiplexor concatenates multiple PPP frames (subframes) into a single, multiplexed frame (superframe). One header is included in the superframe and the individual PPP subframes are separated by delimiters. On the receiving end, a demultiplexor uses the delimiters to separate the individual PPP subframes.

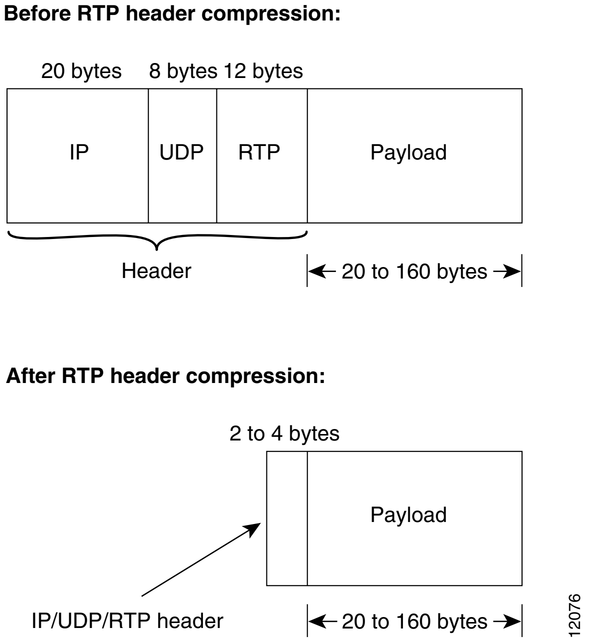
The MGX-RPM-1FE-CP back card conforms to this specification and acts as both a multiplexor and a demultiplexor.

RTP/UDP Header Compression

RTP is a protocol used for carrying packetized audio and video traffic over an IP network. RTP, described in RFC 1889, is not intended for data traffic, which uses TCP or UDP. Instead, RTP provides end-to-end network transport functions intended for applications with real-time requirements (such as audio, video, or simulation data) over multicast or unicast network services.

In an RTP frame, there is a minimum 12 bytes of the RTP header, combined with 20 bytes of IP header, and 8 bytes of UDP header. This creates a 40-byte IP/UDP/RTP header. By comparison, the RTP packet has a payload of approximately 20 to 160 bytes for audio applications that use compressed payloads. Given this ratio, it is very inefficient to transmit the IP/UDP/RTP header without compressing it.

Figure 3 RTP Header Compression



RFCs 2508 and 2509 describe a method for compressing not only the RTP header, but also the associated UDP and IP headers. Using this method, the 40 bytes of header information is compressed into approximately 2 to 4 bytes, as shown in Figure 3. Because the frames are compressed on a link-by-link basis, the delay and loss rate are lower, resulting in improved performance.

The MGX-RPM-1FE-CP back card offloads both the compression and decompression of RTP frames from the RPM-PR.

Note The MGX-RPM-1FE-CP back card can be used to perform only UDP/IP compression, in which case, the header is reduced from 28 bytes to 2 to 4 bytes.

MGX-RPM-1FE-CP Back Card in an IP-RAN

The MGX-RPM-1FE-CP back card off loads the compression/decompression of RTP/UDP headers and the multiplexing/ demultiplexing of PPP frames.

The supported use of the MGX-RPM-1FE-CP back card is within an IP-RAN of a mobile wireless network. In mobile wireless networks, radio coverage over a geographical space is provided by a network of radios and supporting electronics (Base Transceiver Station [BTS]) distributed over a wide area. Each radio and supporting electronics represents a "cell." In traditional networks, the radio signals or radio data frames collected in each cell are forwarded over a T1 (or similar low-speed, leased) line to a centralized Base Station Controller (BSC) where they are processed.

With the blurring of the lines between voice and data, several alternatives have arisen. One alternative is to replace the T1s with a cell- based AAL2/ATM approach to deliver the frames. This alternative seems to work well because the frame sizes within a wireless network match up nicely with the frame sizes used within an ATM network (10-20 bytes).

Another alternative is to encapsulate the radio frames in UDP frames and transport them over an IP network using header compression and packet multiplexing. This alternative provides better bandwidth efficiency than AAL2 and thus greater backhaul capacity. In this alternative, the MGX 8850 is used as a leased line termination and aggregation device. To enable the delivery of the aggregated back haul IP traffic to and from a routed IP network, the MGX is equipped with RPM-PR blades (which terminate and originate the frames) and MGX-RPM-1FE-CP back cards (which compress and multiplex the frames).

The nature of UDP or RTP header compression is such that compressed packets must be decompressed prior to routing. Also, to optimize network bandwidth, the frames must be multiplexed/compressed before they are sent across the T1 line (and decompressed/demultiplexed before they are sent across the FE interface).

- Frames arriving at an FE interface of the MGX-RPM-1FE-CP back card are transferred to the RPM-PR. After the routing decision has been made, the frames are sent to the multiplexing/compression engine, where the PPP frames are multiplexed and the UDP and RTP headers are compressed. The resulting frames are then sent back to the RPM-PR for transmission over the appropriate T1 interface.
- Conversely, frames arriving at a T1 interface of the MGX8850 are transferred to the RPM-PR and then to the decompression/demultiplexing engine. Once the UDP and RTP headers are decompressed and the PPP frames are demultiplexed, the resulting frames are sent back to the RPM-PR so that a routing decision can be made. They are then forwarded to the FE interface.

Multilink PPP (MLP) provides a standardized method for spreading traffic across multiple WAN links, while providing multivendor interoperability, packet fragmentation and proper sequencing, and load-balancing on both inbound and outbound traffic. When used in conjunction with Multilink PPP, the MGX-RPM-1FE-CP back card allows customers to increase channel capacity up to eight T1s.

This solution requires the following components:

- MGX8850
- RPM-PR
- MGX-RPM-1FE-CP back card
- Frame Relay Service Module (FRSM) card
- BTS router (MWR 1941-DC)

The solution uses Open Shortest Path First (OSPF) as the routing protocol and requires MLP for transmission of the packets between the aggregation node (MGX8850) and the BTS. It requires you to configure the following:

- The FE interface to support OSPF. Enable multicast routing and indicate a Protocol Independent Multicast (PIM) mode.
- One or more PPP multilink interfaces with PPP mux and RTP header compression attributes.
- A virtual template for each of the multilink groups.
- A PVC under the switch subinterface that references the virtual template.

In addition, you must configure a connection between the PVC and the FRSM as well as a connection between the FRSM and the PVC.

Supported Platforms

The Cisco MGX-RPM-1FE-CP Back Card is supported in the Cisco MGX 8850/RPM-PR platform.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Configuration Tasks

To configure the MGX-RPM-1FE-CP back card, you must first access the RPM-PR command line interface (CLI). The RPM-PR CLI can be accessed using any of the following three methods:

- Console port on the front of the RPM-PR

  The RPM-PR has an RJ-45 connector on the front of the card module. If you configure the RPM-PR on site, connect a console terminal (an ASCII terminal or a PC running terminal emulation software) directly to the console port on your RPM-PR using an RS-232 to RJ-45 cable for CLI access. The console port is the only way to access the RPM-PR CLI when the card module is first installed into an MGX 8850 chassis.

- Change card (cc) command from another MGX 8850 card

  After initial configuration, you can also configure the RPM-PR through the PXM. You can access the RPM-PR CLI by using the cc (change card) command from any of the other cards in the MGX 8850 switch. The ATM switch interface on the RPM-PR must be enabled before you can use the cc command.

- Telnet from a workstation, PC or another router

  After initial configuration, you can also configure the RPM-PR remotely via telnet. After the RPM-PR is installed and has PVCs to other RPM-PRs or routers in the network, you can telnet to the RPM-PR CLI remotely from these other devices.

For more information about accessing the RPM-PR CLI and the basic Cisco IOS command structure, please see the *RPM Installation and Configuration Guide*.

Configuration of the MGX-RPM-1FE-CP back card requires the following:

- Verifying the Version of IOS Software
- Configuring the FE Interface
- Configuring Multilink Interfaces
- Configuring Virtual Templates
- Configuring the Switch Interface and PVCs
- Saving the Configuration
- Verifying the Configuration

Verifying the Version of IOS Software

The MGX-RPM-1FE-CP back card requires Cisco IOS Release 12.2(8) MC1 or a later Cisco IOS Release 12.2 MC on the corresponding RPM-PR. To verify the version of IOS software, use the **show version** command.

The **show version** command displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

Configuring the FE Interface

To configure the FE interface of the MGX-RPM-1FE-CP back card, complete the following tasks:

- Configuring the FE Interface IP Address
- Setting the Speed and Duplex Mode
- Configuring Routing Protocol Attributes
- Configuring PIM
- Enabling the FE Interface

Configuring the FE Interface IP Address

To configure the FE interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`RPM(config)#` **`interface fastethernet`** *`slot/port`*	Specifies the port adapter type and the location of the interface to be configure. **Note** The *slot* is the slot of the MGX8850 where the RPM-PR resides (upper=1, lower=2). The *port* is the number of the port on the back card.
Step 2	`RPM(config-if)#` **`ip address`** *`ip-address subnet-mask`*	Assigns an IP address and subnet mask to the interface.

Setting the Speed and Duplex Mode

The MGX-RPM-1FE-CP back card can run in full or half duplex mode and at 100 Mbps or 10 Mbps. It also has an auto-negotiation feature that allows the card to negotiate the speed and duplex mode with the corresponding interface on the other end of the connection.

Auto negotiation is the default setting for the speed and transmission mode. However, when using the MGX-RPM-1FE-CP back card in a wireless IP RAN solution, *do not* use auto negotiation. You must explicitly configure a speed of 100 Mbps and either full- or half-duplex transmission mode.

To configure the speed and duplex operation, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	RPM(config-if)# **duplex** [**auto** | **half** | **full**]	Specifies duplex operation.
Step 2	RPM(config-if)# **speed** [**auto** | **100** | **10**]	Specifies speed.

Configuring Routing Protocol Attributes

When used in the IP-RAN solution, the MGX-RPM-1FE-CP back card must be configured to support the OSPF routing protocol.

To configure OSPF routing protocol attributes, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	RPM(config-if)# **ip ospf message-digest-key** *key-id* **md5** *key*	Enables OSPF Message Digest 5 (MD5) authentication.
Step 2	RPM(config-if)# **ip ospf hello-interval** *seconds*	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
Step 3	RPM(config-if)# **ip ospf dead-interval** *seconds*	Sets the interval at which hello packets must not be seen before neighbors declare the router down.

Configuring PIM

Because the MGX-RPM-1FE-CP back card is used in a multicast PPP environment, you should configure the Protocol Independent Multicast (PIM) mode of the FE interface.

To configure the PIM mode, use the following command while in interface configuration mode:

Command	Purpose
RPM(config-if)# **ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}]}	Enables PIM on an interface.

Enabling the FE Interface

To enable the FE interface, use the following command while in interface configuration mode:

Command	Purpose
RPM(config-if)# **no shutdown**	Enables the interface.

Configuring Multilink Interfaces

To configure the multilink interfaces to be used in conjunction with the MGX-RPM-1FE-CP back card, complete the following tasks:

- Configuring the Loopback Interface
- Configuring Multilink PPP
- Configuring IP Address Assignment
- Configuring PPP Multiplexing
- Configuring RTP/UDP Compression
- Configuring Routing Protocol Attributes
- Configuring PIM

Configuring the Loopback Interface

The loopback interface is a software-only, virtual interface that emulates an interface that is always up. The interface-number is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.

Because the multilink interface is a virtual interface, you should create a loopback interface for the multilink interface to enable IP processing on the interface without having to assign an explicit IP address.

To configure a loopback interface for the multilink interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`RPM(config)# interface loopback number`	Creates a loopback interface for the multilink interface.
Step 2	`RPM(config-if)# ip address ip-address subnet-mask`	Assigns an IP address and subnet mask to the interface.
Step 3	`RPM(config-if)# exit`	Exits interface configuration mode.

Configuring Multilink PPP

As higher-speed services are deployed, Multilink-PPP (MLP) provides a standardized method for spreading traffic across multiple WAN links, while providing multivendor interoperability, packet fragmentation and proper sequencing, and load balancing on both inbound and outbound traffic. The MGX-RPM-1FE-CP back card used in conjunction with the Multilink Point-to-Point Protocol (PPP) feature provides customers with the ability to increase channel capacity to up to eight T1s.

A Multilink interface is a special virtual interface which represents a multilink PPP bundle. The multilink interface serves to coordinate the configuration of the bundled link, and presents a single object for the aggregate links. However, the individual PPP links that are aggregated together, must also be configured. Therefore, to enable Multilink PPP on multiple serial interfaces, you need to first set up the multilink interface, and then configure each of the serial interfaces and add them to the same multilink interface.

To set up the multilink interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`RPM(config)#` **`interface multilink`** *`number`*	Specifies the multilink interface to be configured.
Step 2	`RPM(config-if)#` **`ppp multilink`**	Enables multilink PPP operation.
Step 3	`RPM(config-if)#` **`no ppp multilink fragmentation`**[1] or `RPM(config-if)# ppp multilink fragment disable`[2]	Disables PPP multilink fragmentation.
Step 4	`RPM(config-if)#` **`multilink-group`** *`group-`*`number`[1] or `RPM(config-if)#` **`ppp multilink group`** *`group-`*`number`[2]	Specifies an identification number for the multilink interface.
Step 5	`RPM(config-if)#` **`ip unnumbered loopback`** *`number`*	Enables IP processing on the multilink interface without assigning an explicit IP address to the interface, where *number* is the number of the loopback interface that you configured in Configuring the Loopback Interface.

[1] Cisco IOS Release 12.2(15)MC2a or later.

[2] Cisco IOS 12.3(11)T or later.

Configuring IP Address Assignment

A point-to-point interface must be able to provide a remote node with its IP address through the IP Control Protocol (IPCP) address negotiation process. The IP address can be obtained from a variety of sources. The address can be configured through the command line, entered with an EXEC-level command, provided by TACACS+ or the Dynamic Host Configuration Protocol (DHCP), or from a locally administered pool.

IP address pooling uses a pool of IP addresses from which an incoming interface can provide an IP address to a remote node through IPCP address negotiation process. IP address pooling also enhances configuration flexibility by allowing multiple types of pooling to be active simultaneously.

To configure the an IP address assignment, use the following command while in interface configuration mode:

Command	Purpose
`RPM(config-if)#` **`peer default ip address`** `{`*`ip-address`* `|` **`dhcp`** `|` **`pool`** `[`*`pool-name`*`]}`	Specifies an IP address, an address from a specific IP address pool, or an address from the Dynamic Host Configuration Protocol (DHCP) mechanism to be returned to a remote peer connecting to this interface.

Configuring PPP Multiplexing

To enable and control the multiplexing of PPP frames, use the following commands while still in multilink interface configuration mode:

To enable and control the multiplexing of PPP frames, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#` **`ppp mux`**	Enables PPP multiplexing.
Step 2	`RPM(config-if)#` **`ppp mux delay`** *`integer`*	Sets the maximum time delay.
Step 3	`RPM(config-if)#` **`ppp mux subframe length`** *`integer`*	Sets the maximum length of the subframe.
Step 4	`RPM(config-if)#` **`ppp mux frame`** *`integer`*	Sets the maximum length of the superframe
Step 5	`RPM(config-if)#` **`ppp mux subframe count`** *`integer`*	Sets the maximum number of subframes in a superframe.
Step 6	`RPM(config-if)#` **`ppp mux pid`** *`integer`*	Sets the default PPP protocol ID.

Configuring ACFC and PFC Handling During PPP Negotiation

With Cisco IOS Release 12.2(15)MC1 and later, ACFC and PFC handling during PPP negotiation can be configured. By default, ACFC/PFC handling is not enabled.

To configure ACFC handling during PPP negotiation, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#` **`ppp acfc remote`** `{`**`apply`** `|` **`reject`** `|` **`ignore`**`}`	Configures how the router handles the ACFC option in configuration requests received from a remote peer, where: • **apply**—ACFC options are accepted and ACFC may be performed on frames sent to the remote peer. • **reject**—ACFC options are explicitly ignored. • **ignore**—ACFC options are accepted, but ACFC is not performed on frames sent to the remote peer.
Step 2	`RPM(config-if)#` **`ppp acfc local`** `{`**`request`** `|` **`forbid`**`}`	Configures how the router handles ACFC in its outbound configuration requests, where: • **request**—The ACFC option is included in outbound configuration requests. • **forbid**—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.

To configure PFC handling during PPP negotiation, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#` **`ppp pfc remote`** `{`**`apply`** `|` **`reject`** `|` **`ignore`**`}`	Configures how the router handles the PFC option in configuration requests received from a remote peer, where: • **apply**—PFC options are accepted and PFC may be performed on frames sent to the remote peer. • **reject**—PFC options are explicitly ignored. • **ignore**—PFC options are accepted, but PFC is not performed on frames sent to the remote peer.
Step 2	`RPM(config-if)#` **`ppp pfc local`** `{`**`request`** `|` **`forbid`**`}`	Configures how the router handles PFC in its outbound configuration requests, where: • **request**—The PFC option is included in outbound configuration requests. • **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.

Configuring RTP/UDP Compression

Enabling RTP/UDP compression (cRTP/cUDP) on both ends of a low-bandwidth serial link can greatly reduce the network overhead if there is a lot of RTP traffic on that slow link. This compression is beneficial especially when the RTP payload size is small (for example, compressed audio payloads of 20-50 bytes).

Note Before you can enable RTP header compression, you must configure a serial line that uses PPP encapsulation.

To configure RTP header compression when using Cisco IOS Release 12.2(15)MC2a or prior, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#` **`ip rtp header-compression`**	Enables RTP header compression for serial encapsulations.
Step 2	`RPM(config-if)#` **`ip rtp compression-connections`** *`number`*	Configures the total number of RTP header compression connections on an interface. By default, a total of 16 RTP compression connections on an interface is supported.

To configure RTP header compression when using Cisco IOS Release 12.3(11)T or later, use the following commands while in multilink interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)# ip rtp header-compression ignore-id`	Enables RTP header compression for serial encapsulations and suppresses IP ID checking during RTP compression.
Step 2	`RPM(config-if)# ip rtp compression-connections number`	Configures the total number of RTP header compression connections on an interface. By default, a total of 16 RTP compression connections on an interface is supported.

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.

Configuring the RTP/UDP Compression Flow Expiration Timeout Duration

To minimize traffic corruption, cUDP flows expire after a period of time during which no packets are passed. When this user defined duration of inactivity occurs on a flow at the compressor, the compressor sends a full header upon receiving a packet for that flow, or, if no new packet is received for that flow, the compressor makes the CID for the flow available for new use. When a packet is received at the decompressor after the duration of inactivity has been exceeded, the packet is dropped and a context state message is sent to the compressor requesting a flow refresh.

The default expiration timeout is 5 seconds. The recommended value is 8 seconds.

Caution Failure of performance/latency scripts could occur if the expiration timeout duration is not changed to the recommended 8 seconds.

To configure the duration of the cUDP flow expiration timeout, use the following command while in multilink interface configuration mode:

Command	Purpose
`RPM(config-if)# ppp iphc max-time seconds`	Specifies the duration of inactivity, in seconds, that when exceeded causes the cUDP flow to expire.

Configuring Routing Protocol Attributes

When used in the IP-RAN solution, the multilink interface must be configured to support the OSPF routing protocol.

To configure OSPF routing protocol attributes, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#` **`ip ospf message-digest-key`** *`key-id`* **`md5`** *`key`*	Enables OSPF Message Digest 5 (MD5) authentication.
Step 2	`RPM(config-if)#` **`ip ospf hello-interval`** *`seconds`*	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
Step 3	`RPM(config-if)#` **`ip ospf dead-interval`** *`seconds`*	Sets the interval at which hello packets must not be seen before neighbors declare the router down.

Configuring PIM

Because the MGX-RPM-1FE-CP back card is used in a multicast PPP environment, you should configure the Protocol Independent Multicast (PIM) mode of the multilink interface.

To configure the PIM mode, use the following command while in interface configuration mode:

Command	Purpose
`RPM(config-if)#` **`ip pim`** `{`**`sparse-mode`** `|` **`sparse-dense-mode`** `|` **`dense-mode`** `[`**`proxy-register`** `{`**`list`** *`access-list`* `|` **`route-map`** *`map-name`*`}]}`	Configures PIM on an interface, where: • **sparse-mode**—Enables sparse mode of operation. • **sparse-dense-mode**—Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in. • **dense-mode**—Enables dense mode of operation. • **proxy-register**—(Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR. • **list** *access-list*—(Optional) Defines the extended access list number or name. • **route-map** *map-name*—(Optional) Defines the route map.

Configuring Virtual Templates

To configure the virtual templates to be used in conjunction with the MGX-RPM-1FE-CP back card, complete the following tasks:

- Configuring the IP Address
- Configuring Multilink PPP
- Enabling Link Quality Monitoring (LQM)

Configuring the IP Address

No IP address should be associated with the virtual template.

To configure no IP address, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	RPM(config)# **interface virtual-template** *number*	Specifies the virtual template interface to be configured.
Step 2	RPM(config-if)# **no ip address**	Indicates that no IP address is associated with the virtual template.

Configuring Multilink PPP

To associate the virtual template with a multilink group, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	RPM(config-if)# **ppp multilink**	Enables multilink PPP operation.
Step 2	RPM(config-if)# **ppp multilink queue depth qos** *number*	Specifies link queueing parameters.This command sets the maximum depth for link queues when a bundle has non-FIFO queuing. The possible values are 2 through 255.
Step 3	RPM(config-if)# **multilink-group** *group-number*[1] or RPM(config-if)# **ppp multilink group** *group-number*[2]	Specifies an identification number for the multilink interface.

[1] Cisco IOS Release 12.2(15)MC2a or prior.

[2] Cisco IOS Release 12.3(11)T or later.

Enabling Link Quality Monitoring (LQM)

Link Quality Monitoring (LQM) is available on all serial interfaces running PPP. LQM will monitor the link quality, and if the quality drops below a configured percentage, the router shuts down the link. The percentages are calculated for both the incoming and outgoing directions. The outgoing quality is calculated by comparing the total number of packets and bytes sent with the total number of packets and bytes received by the destination node. The incoming quality is calculated by comparing the total number of packets and bytes received with the total number of packets and bytes sent by the destination peer.

When LQM is enabled, Link Quality Reports (LQRs) are sent, in place of keepalives, every keepalive period. All incoming keepalives are responded to properly. If LQM is not configured, keepalives are sent every keepalive period and all incoming LQRs are responded to with an LQR.

Note LQR is specified in RFC 1989, *PPP Link Quality Monitoring*, by William A. Simpson of Computer Systems Consulting Services.

To enable LQM on the interface, use the following command while in interface configuration mode:

Command	Purpose
`RPM(config-if)# ppp quality percentage`	Sets the link quality threshold. The *percentage* argument specifies the link quality threshold. That percentage must be maintained, or the link is deemed to be of poor quality and taken down.

Configuring the Switch Interface and PVCs

To configure the switch interface and the permanent virtual circuits (PVCs) to be used in conjunction with the MGX-RPM-1FE-CP back card, complete the following tasks:

- Configuring the IP Address
- Configuring the PVC

Configuring the IP Address

No IP address should be associated with the switch interface. To configure no IP address, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`RPM(config)# interface switch number`	Specifies the switch interface to be configured.
Step 2	`RPM(config-if)# no ip address`	Indicates that no IP address is associated with the switch interface.

Configuring the PVC

To configure a permanent virtual circuit (PVC) on a switch subinterface, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	`RPM(config-if)#` **`interface Switch`** *`number.subinterface`* **`point-to-point`**	Specifies the switch subinterface.
Step 2	`RPM(config-if)#` **`pvc`** *`vpi`*`/`*`vci`*	Specifies the PVC to be configured.
Step 3	`RPM(config-if)#` **`encapsulation aal5`** *`encap`* `[`**`virtual-template`** *`number`*`]`	Specifies the ATM adaptation layer (AAL) and encapsulation type for the PVC and to associate the PVC with a virtual template.

Saving the Configuration

To save the configuration, use the following command while in global configuration mode:

Command	Purpose
`RPM#` **`copy running-config startup-config`**	Writes the new configuration to nonvolatile memory.

Verifying the Configuration

To verify the configuration of the PPP multiplexing and the cRTP/cUDP compression on the MGX-RPM-1FE-CP back card, enter the following command:

```
RPM# show running-config
```

Monitoring and Maintaining the MGX-RPM-1FE-CP Back Card

The following privilege EXEC commands can be used to monitor and maintain multilink and FE interfaces, and to view information about the PPP mux and header compression configuration:

Command	Purpose
`RPM#` **`clear counters fastethernet`** *`slot`*`/`*`port`*	Clears interface counters.
`RPM#` **`clear ip rtp header-compression`**	Clears RTP header compression structures and statistics.
`RPM#` **`clear ppp mux`** *`interface`*	Clears the PPP multiplexing interface counters.
`RPM#` **`show ppp multilink`**	Displays MLP and multilink bundle information.
`RPM#` **`show ppp multilink interface`** *`number`*	Displays multilink information for the specified interface.

Command	Purpose
`RPM# show interfaces fastethernet slot/port`	Displays the status of the FE interface.
`RPM# show ppp mux interface interface`	Displays statistics for PPP frames that have passed through a given multilink interface.
`RPM# show ip rtp header-compression`	Displays RTP header compression statistics.
`RPM# show controllers fastethernet slot/port`	Displays information about initialization block, transmit ring, receive ring and errors for the Fast Ethernet controller chip.

Enabling Remote Management of the MGX-RPM-1FE-CP Back Card

You can use Cisco's network management applications, such as Cisco Works for Mobile Wireless (CW4MW), to monitor and manage aspects of the MGX-RPM-1FE-CP back card.

To enable remote network management of the MGX-RPM-1FE-CP back card, do the following:

Step 1 At the privileged prompt, enter the following command to access configuration mode:

```
RPM# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RPM(config)#
```

Step 2 At the configuration prompt, enter the following command to assign a host name to each of the network management workstations:

```
RPM(config)# ip host hostname ip-address
```

Where *hostname* is the name assigned to the Operations and Maintenance (O&M) workstation and *ip-address* is the address of the network management workstation.

Step 3 Enter the following command to log messages to a syslog server host:

```
RPM(config)# logging hostname
```

Where *hostname* is the name assigned to the CW4MW workstation with the **ip host** command.

Step 4 Enter the following commands to create a loopback interface for O&M:

```
RPM(config)# interface loopback number
RPM(config-if)# ip address ip-address subnet-mask
```

Step 5 Exit interface configuration mode:

```
RPM(config-if)# exit
```

Step 6 At the configuration prompt, enter the following command to specify the recipient of a Simple Network Management Protocol (SNMP) notification operation:

```
RPM(config)# snmp-server host hostname [traps | informs] [version {1 | 2c | 3 [auth |
noauth | priv]}] community-string [udp-port port] [notification-type]
```

Where *hostname* is the name assigned to the CW4MW workstation with the **ip host** command in Step 2.

Step 7 Enter the following commands to specify the public and private SNMP community names:

```
RPM(config)# snmp-server community public RO
RPM(config)# snmp-server community private RW
```

Step 8 Enter the following command to enable the sending of SNMP traps:

```
RPM(config)# snmp-server enable traps
```

Step 9 Enter the following command to specify the loopback interface from which SNMP traps should originate:

```
RPM(config)# snmp-server trap-source loopback number
```

Where *number* is the number of the loopback interface you configured for the O&M in Step 4.

Step 10 At the configuration prompt, press Ctrl-Z to exit configuration mode.

Step 11 Write the new configuration to nonvolatile memory as follows:

```
RPM# copy running-config startup-config
```

Related Documentation

This following documents contain important information related to the MGX-RPM-1FE-CP back card:

- *Cisco MGX-RPM-1FE-CP Back Card Installation and Configuration Note*
- *Release Notes for the MGX-RPM-1FE-CP Back Card*
- *Cisco MGX 8850 Hardware Installation Guide*