



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

The 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

© <year> Cisco Systems, Inc. All rights reserved.

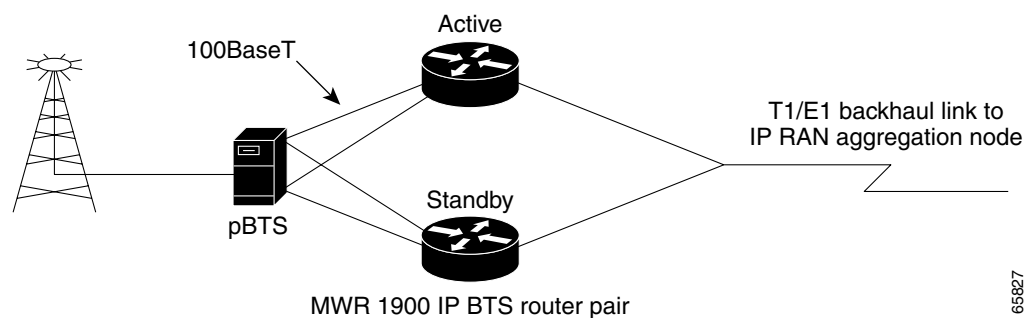
Feature Overview

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 1941-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.

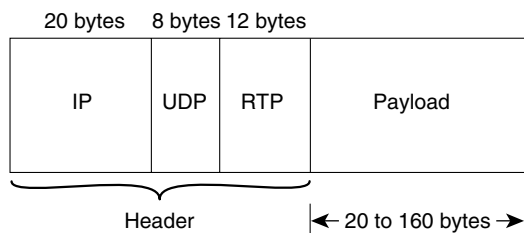
RTP/UDP Header Compression

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.

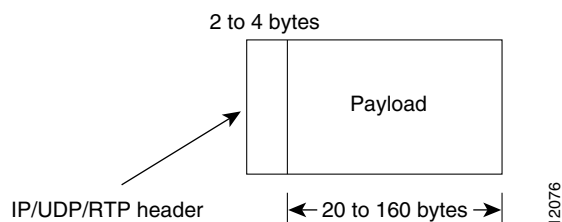
In an RTP frame, there is a minimum 12 bytes of the RTP header, combined with 20 bytes of IP header, and 8 bytes of UDP header. This creates a 40-byte IP/UDP/RTP header. By comparison, the RTP packet has a payload of approximately 20 to 160 bytes for audio applications that use compressed payloads. Given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

Figure 2 RTP Header Compression

Before RTP header compression:



After 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 1941-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/specgdl/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: <i>password</i> 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 Router(config-line)# exec-timeout 0 0 Router(config-line)# exit Router(config)#	Enter line configuration mode to configure the console port. When you enter line configuration mode, the prompt changes to Router(config-line)#. Prevent the router's EXEC facility from timing out if you do not type any information on the console screen for an extended period. 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 <i>number</i>	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 <i>ip-address subnet-mask</i>	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 <i>slot/port</i>	Specifies the port adapter type and the location of the interface to be configured. The <i>slot</i> is always 0 and the <i>port</i> is the number of the port (0 or 1).
Step 2	Router(config-if)# ip address <i>ip-address subnet-mask</i>	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 <i>key-id</i> md5 <i>key</i>	Enables OSPF Message Digest 5 (MD5) authentication.
Step 2	Router(config-if)# ip ospf hello-interval <i>seconds</i>	Configures the interval between hello packets that the Cisco IOS software sends on the interface.
Step 3	Router(config-if)# ip ospf dead-interval <i>seconds</i>	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
<pre>Router(config-if)# ip pim {sparse-mode sparse-dense-mode dense-mode [proxy-register {list access-list route-map map-name}]}</pre>	<p>Configures PIM on an interface, where:</p> <ul style="list-style-type: none"> • 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 Standby 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 HSRP, use the following commands while in interface configuration mode:

	Command	Purpose
Step 1	Router(config-if)# standby group name <i>group-name</i>	<p>Specifies the name of the standby group.</p> <p>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.</p> <p>Tip If you omit the <i>group-name</i> 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.</p>
Step 2	Router(config-if)# standby group ip <i>address</i>	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] <i>hellotime</i> [msec] <i>holdtime</i>	<p>Configures the time between hello packets and the time before other routers declare the active Hot Standby or standby router to be down.</p> <p>Note You <i>must</i> use 1 for the hello time and 3 for the hold time.</p>
Step 4	Router(config-if)# standby group preempt	<p>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.</p> <p>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.</p>

Configuring Tasks

	Command	Purpose
Step 5	<pre>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</pre>	<p>Specifies other interfaces on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group.</p> <p>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.</p> <p>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 <i>must</i> be as follows: 10 for the multilink, FE, and health interfaces; 5 for the revertive interface.</p>
Step 6	<pre>Router(config-if)# standby group priority 100</pre>	<p>Configures HSRP priority.</p> <p>Note We recommend that you specify a priority of 100.</p>



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
<pre>Router(config-if)# no shutdown</pre>	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 <i>number</i>	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 <i>group-number</i> ¹ OR RPM(config-if)# ppp multilink group <i>group-number</i> ²	Specifies an identification number for the multilink interface.
Step 4	RPM(config-if)# ip unnumbered loopback <i>number</i>	Enables IP processing on the multilink interface without assigning an explicit IP address to the interface, where <i>number</i> 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 { <i>ip-address</i> dhcp pool [<i>pool-name</i>]}	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 <i>integer</i>	Sets the maximum time delay.
Step 3	RPM(config-if)# ppp mux subframe length <i>integer</i>	Sets the maximum length of the subframe.
Step 4	RPM(config-if)# ppp mux frame <i>integer</i>	Sets the maximum length of the superframe
Step 5	RPM(config-if)# ppp mux subframe count <i>integer</i>	Sets the maximum number of subframes in a superframe.
Step 6	RPM(config-if)# ppp mux pid <i>integer</i>	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 <i>number</i>	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 <i>number</i>	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 <i>seconds</i>	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 <i>key-id</i> md5 <i>key</i>	Enables OSPF Message Digest 5 (MD5) authentication.
Step 2	RPM(config-if)# ip ospf hello-interval <i>seconds</i>	Specifies the interval between hello packets that the Cisco IOS software sends on the interface.
Step 3	RPM(config-if)# ip ospf dead-interval <i>seconds</i>	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 <i>access-list</i> route-map <i>map-name</i> }]}	Configures PIM on an interface, where: <ul style="list-style-type: none"> • 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 <i>access-list</i>—(Optional) Defines the extended access list number or name. • route-map <i>map-name</i>—(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 <i>ip-address subnet-mask</i>	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 [<i>period</i> [<i>retries</i>]]	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 <i>number</i>	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 <i>slot/port</i>	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] <i>class-name</i>	<p>Assigns a name to your class map, where:</p> <ul style="list-style-type: none"> 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 <p>When you enter the class-map command, you are placed in class map configuration mode.</p>
Step 2	Router(config-cmap)# match access-group <i>number</i> Router(config-cmap)# match ip dscp <i>number</i> Router(config-cmap)# match ip precedence <i>number</i> Router(config-cmap)# match input-interface <i>interface-name</i> Router(config-cmap)# match protocol <i>protocol</i>	<p>Describes the characteristics of the packets that are subject to QoS (can use one or more):</p> <ul style="list-style-type: none"> 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. <p>Note For more information about these commands, see the <i>Cisco IOS Quality of Service Solutions Command Reference</i>.</p>
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 <i>policy-name</i>	<p>Assigns a name to your policy map.</p> <p>When you enter the policy-map command, you are placed in policy map configuration mode.</p>
Step 2	Router(config-pmap)# class <i>class-name</i>	<p>Associates the policy map with a class map.</p> <p>Specify the same <i>class-name</i> 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.</p>
Step 3	<pre>Router(config-pmap-c)# priority percent <i>number</i> Router(config-pmap-c)# bandwidth percent <i>number</i> Router(config-pmap-c)# queue-limit <i>number</i> Router(config-pmap-c)# priority <i>rate-in-kbps</i> Router(config-pmap-c)# shape {average peak} <i>cir</i> [<i>bc</i>] [<i>be</i>] Router(config-pmap-c)# shape max-buffers <i>number-of-buffers</i></pre>	<p>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):</p> <ul style="list-style-type: none"> • 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 queuing 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. <p>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.</p> <p>For more information about these commands, see the <i>Cisco IOS Quality of Service Solutions Command Reference</i>.</p>

	Command	Purpose
Step 4	<pre>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</pre>	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>For more information about these commands, see the “<i>Cisco IOS Quality of Service Solutions Command Reference</i>.”</p>
Step 5	<pre>Router(config-pmap-c)# exit</pre>	Exits the class submode of the policy map configuration mode. Repeat Step 2 and Step 3 for each class map.
Step 6	<pre>Router(config-pmap)# exit</pre>	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	<pre>Router(config)# interface multilink number</pre>	Accesses the multilink interface configuration mode.
Step 2	<pre>Router(config-if)# service-policy output policy-name</pre>	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 **disable-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 used 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 the **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; **span 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 subframe 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

The 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

