



## **Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide**

July 2009

### **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

Text Part Number: OL-18665-01

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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

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

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcom the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bring the Meeting To You, Catalyst, CCDA, CDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow M Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

*Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide*

Copyright © 2009, Cisco Systems, Inc.

All rights reserved. Printed in USA.



# CONTENTS

## About This Guide vii

Document Revision History vii

Objectives vii

Audience viii

Organization viii

Conventions viii

Related Documentation ix

Obtaining Documentation, Obtaining Support, and Security Guidelines x

## Cisco MWR 2941-DC Router Overview 1-1

Introduction 1-1

RAN Transport Solutions 1-2

Features 1-2

Cisco Pseudowire Emulation Edge-to-Edge 1-2

GSM Abis Optimization over IP Implementation 1-4

Bidirectional Forwarding Detection 1-5

Intelligent Cell Site IP Services 1-5

RAN-Optimization Implementation 1-6

Cisco IOS Software Features 1-6

Software Features 1-7

Configuration Statements for CISCO-IP-RAN-BACKHAUL-MIB 1-7

Network Management Features 1-10

Cisco Mobile Wireless Transport Manager (MWTM) 1-10

MIB Support 1-11

Limitations and Restrictions 1-11

Hardware Limitations and Restrictions 1-11

Software Limitations and Restrictions 1-12

New Features in Cisco IOS Release 12.4(19)MR2 1-12

## Cisco IOS Software Basics 2-1

Getting Help 2-1

Understanding Command Modes 2-1

Undoing a Command or Feature 2-2

Saving Configuration Changes 2-3

## First-Time Configuration 3-1

Understanding the Cisco MWR 2941-DC Router Interface Numbering 3-1

Slot and Port Numbering 3-2

Setup Command Facility 3-3

Before Starting Your Router 3-3

Using the Setup Command Facility 3-3

Configuring Global Parameters 3-3

Completing the Configuration 3-6

## Configuring the Cisco MWR 2941-DC Router Using the CLI 4-1

Verifying the Cisco IOS Software Version 4-1

Configuration Sequence 4-1

Configuring the Hostname and Password 4-2

Verifying the Hostname and Password 4-3

Configuring Gigabit Ethernet Interfaces 4-4

Configuring Network Clocking Support 4-6

Configuring Pseudowire 4-13

Configuring MLPPP Backhaul 4-22

Configuring GSM-Abis Links 4-31

Configuring SNMP Support 4-33

Configuring ATM IMA 4-37

Configuring BFD 4-39

Configuring Satellite Support in a RAN-O Network 4-40

Configuring Graceful Degradation 4-42

Configuring Link Noise Monitor 4-43

Saving Configuration Changes 4-45

Monitoring and Managing the Cisco MWR 2941-DC Router 4-46

Using Cisco Mobile Wireless Transport Manager (MWTM) 4-46

Enabling the Cisco MWR 2941-DC Router for Remote Network Management 4-46

Show Commands for Monitoring the Cisco MWR 2941-DC Router 4-48

## APPENDIX A

### Cisco MWR 2941-DC Router Command Reference A-1

## APPENDIX B

### Configuration Examples B-1

Examples B-1

Asymmetric PWE3 Configuration B-2

PWE3 Redundancy Configuration B-15

TDM over MPLS Configuration	B-21
ATM over MPLS Configuration	B-25
GSM-Only Configuration	B-32
GSM-Only Configuration Using Satellite	B-36
GSM Congestion Management	B-39

---

**INDEX**





## About This Guide

---

This section describes the objectives, audience, organization, and conventions of this software configuration guide. It contains the following sections:

- [Document Revision History, page vii](#)
- [Objectives, page vii](#)
- [Audience, page viii](#)
- [Organization, page viii](#)
- [Conventions, page viii](#)
- [Related Documentation, page ix](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page x](#)

## Document Revision History

The Document Revision History table below records technical changes to this document.

Document Number	Date	Change Summary
OL-18665-01	July 2009	Added <a href="#">Configuring Link Noise Monitor, page 43</a> .
OL-18665-01	June 2009	Added the following sections: <ul style="list-style-type: none"><li>• <a href="#">Bidirectional Forwarding Detection, page 5</a></li><li>• <a href="#">Configuring Pseudowire, page 13</a></li><li>• <a href="#">Configuring BFD for OSPF, page 39</a></li></ul>
OL-18665-01	March 2009	Initial release.

## Objectives

This guide explains how to configure features that enable the Cisco MWR 2941-DC mobile wireless router to be implemented in an radio access network optimization (RAN-O).

# Audience

This publication is for the person responsible for configuring the router. This guide is intended for the following audiences:

- Customers with technical networking background and experience
- System administrators who are familiar with the fundamentals of router-based internetworking, but who may not be familiar with Cisco IOS software
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software

# Organization

The major sections of this software configuration guide are listed in the following table:

Chapter	Title	Description
Chapter 1	<a href="#">Cisco MWR 2941-DC Router Overview</a>	Describes the purpose of the Cisco MWR 2941-DC router and its unique software features.
Chapter 2	<a href="#">Cisco IOS Software Basics</a>	Describes what you need to know about the Cisco IOS software.
Chapter 3	<a href="#">First-Time Configuration</a>	Describes how to use the setup command facility to configure basic attributes of your router.
Chapter 4	<a href="#">Configuring the Cisco MWR 2941-DC Router Using the CLI</a>	Describes how to use the Cisco IOS software command-line interface (CLI) to configure basic router functionality.
Appendix A	<a href="#">Cisco MWR 2941-DC Router Command Reference</a>	Provides information about new and changed commands.
Appendix B	<a href="#">Configuration Examples</a>	Provides examples of configurations.
Index		

# Conventions

This publication uses the following conventions to convey instructions and information.

Convention	Description
<b>boldface font</b>	Commands and keywords.
<i>italic font</i>	Variables for which you supply values.
[    ]	Keywords or arguments that appear within square brackets are optional.
{ x   y   z }	A choice of required keywords appears in braces separated by vertical bars. You must select one.
screen font	Examples of information displayed on the screen.
<b>boldface screen font</b>	Examples of information the user enters.



Convention	Description
< >	Nonprinting characters, for example passwords, appear in angle brackets.
[ ]	Default responses to system prompts appear in square brackets.

**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.

**Tip**

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

**Caution**

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

## Related Documentation

The following list includes documentation related to your product by implementation.

### Cisco Mobile Wireless RAN Optimization

- Cisco MWR 2941-DC Mobile Wireless Edge Router Documents
  - *Cisco MWR-2941-DC Mobile Wireless Edge Router Hardware Installation Guide*
  - *Cisco MWR-2941-DC Mobile Wireless Edge Router Rack Mounting Instructions*
  - *Regulatory Compliance and Safety Information for the Cisco MWR-2941-DC Mobile Wireless Edge Router*
- Cisco Interface Cards Installation Guides
  - *Quick Start Guide: Interface Cards*
  - Cisco Interface Cards Installation Guide
- Release Notes
  - *Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router*

**Note**

To obtain the latest information, access the online documentation.

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



# CHAPTER 1

## Cisco MWR 2941-DC Router Overview

---

The Cisco MWR 2941-DC Mobile Wireless Router is a cell-site access platform specifically designed to optimize, aggregate, and transport mixed-generation radio access network (RAN) traffic. The router is used at the cell site edge as a part of a 2G, 3G, or 4G radio access network (RAN).

The Cisco MWR 2941-DC helps enable a variety of RAN solutions by extending IP connectivity to devices using Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Node Bs using HSPA or LTE, base transceiver stations (BTSs) using Enhanced Data Rates for GSM Evolution (EDGE), Division Multiple Access (CDMA), CDMA-2000, EVDO, or WiMAX, and other cell-site equipment. It transparently and efficiently transports cell-site voice, data, and signaling traffic over IP using traditional T1/E1 circuits, including leased line, microwave, and satellite, as well as alternative backhaul networks, including Carrier Ethernet, DSL, Ethernet in the First Mile (EFM), and WiMAX. It also supports standards-based Internet Engineering Task Force (IETF) Internet protocols over the RAN transport network, including those standardized at the Third-Generation Partnership Project (3GPP) for IP RAN transport.

Custom designed for the cell site, the Cisco MWR 2941-DC features a small form factor, extended operating temperature, and cell-site DC input voltages.

This chapter includes the following sections:

- [Introduction, page 1-1](#)
- [Cisco IOS Software Features, page 1-6](#)
- [MIB Support, page 1-11](#)
- [Limitations and Restrictions, page 1-11](#)
- [New Features in Cisco IOS Release 12.4\(19\)MR2, page 1-12](#)

## Introduction

A typical RAN is composed of thousands of base transceiver stations (BTSs)/Node Bs, hundreds of base station controllers/radio network controllers (BSCs/RNCs), and several mobile switching centers (MSCs). The BTS/Node Bs and BSC/RNC are often separated by large geographic distances, with the BTSs/Node Bs located in cell sites uniformly distributed throughout a region, and the BSCs, RNCs, and MSCs located at suitably chosen Central Offices (CO) or mobile telephone switching offices (MTSO).

The traffic generated by a BTS/Node B is transported to the corresponding BSC/RNC across a network, referred to as the backhaul network, which is often a hub-and-spoke topology with hundreds of BTS/Node Bs connected to a BSC/RNC by point-to-point time division multiplexing (TDM) trunks. These TDM trunks may be leased-line T1/E1s or their logical equivalents, such as microwave links or satellite channels.

## RAN Transport Solutions

The Cisco MWR 2941-DC Mobile Wireless Router supports a variety of RAN transport solutions, including the following:

- Optimized RAN transport over IP: Maximizes voice and data call density per T1/E1 over the RAN transport network for standards including GSM, GPRS, EDGE, HSPA, and fourth-generation (4G). Optimization helps reduce backhaul transmission costs, which are typically the largest operational expenses in the network.
- IP/Multiprotocol Label Switching (MPLS) RAN backhaul: Allows you to create a high-speed backhaul for a variety of traffic types, including GSM, CDMA, HSPA/LTE, CDMA, EVDO, and WiMAX networks.
- Cell-site operations support networks: Facilitates telemetry to cell sites for remote operations and network element management.
- Cell-site IP points of presence (POPs): Allows you to offer IP services and applications at cell sites.

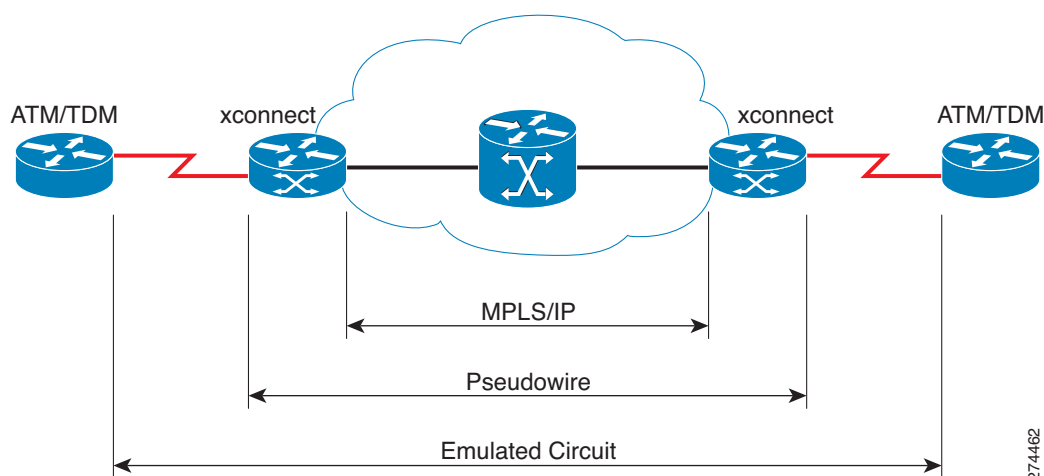
## Features

The following sections describe the features available in the Cisco MWR 2941-DC router.

### Cisco Pseudowire Emulation Edge-to-Edge

Cisco Pseudowire Emulation Edge-to-Edge (PWE3) is a mechanism that emulates the essential attributes of a service, such as EI/T1 ([Figure 1-1](#)).

**Figure 1-1** Cisco MWR 2941-DC Router in a PWE3—Example



The required functions of pseudowires (PWs) include encapsulating service-specific packet data units (PDUs) arriving at an ingress port and carrying them across a path or tunnel, managing their timing and order, and other operations required to emulate the behavior of the service efficiently.

PW is perceived as an unshared link or circuit of the chosen service. However, there may be deficiencies that impede some applications from being carried on a PW. These limitations should be fully described in the appropriate service-specific documents and applicability statements.

Cisco supports standards-based PWE3 as defined by:

- [Structure-agnostic TDM over Packet, page 1-3](#)
- [Structure-aware TDM Circuit Emulation Service over Packet-Switched Network, page 1-3](#)
- [Transportation of Service Using ATM over MPLS, page 1-3](#)

A PW is a connection between two provider edge (PE) devices, which connects two attachment circuits (ACs). An AC can be a VPI/VCI or an T1/E1 link.

## Structure-agnostic TDM over Packet

SAToP encapsulates TDM bit-streams (T1, E1, T3, E3) as PWs over PSNs. It disregards any structure that may be imposed on streams, in particular the structure imposed by the standard TDM framing.

The protocol used for emulation of these services does not depend on the method in which attachment circuits are delivered to the PEs. For example, a T1 attachment circuit is treated the same way for all delivery methods, including: PE on copper, multiplex in a T3 circuit, mapped into a virtual tributary of a SONET/SDH circuit, or carried over a network using unstructured Circuit Emulation Service (CES). Termination of specific carrier layers used between the PE and circuit emulation (CE) is performed by an appropriate network service provider (NSP).

For instructions on how to configure SAToP, see [Configuring Structure-Agnostic TDM over Packet \(SAToP\), page 4-15](#). For a sample SAToP configuration, see [TDM over MPLS Configuration, page B-21](#).

## Structure-aware TDM Circuit Emulation Service over Packet-Switched Network

CESoPSN encapsulates structured (NxDS0) TDM signals as PWs over PSNs. It complements similar work for structure-agnostic emulation of TDM bit-streams, such as PWE3-SAToP.

Emulation of NxDS0 circuits saves PSN bandwidth and supports DS0-level grooming and distributed cross-connect applications. It also enhances resilience of CE devices due to the effects of loss of packets in the PSN.

For instructions on how to configure SAToP, see [Configuring Circuit Emulation Service over Packet-Switched Network \(CESoPSN\), page 4-15](#). For a sample CESoPSN configuration, see [TDM over MPLS Configuration, page B-21](#).

## Transportation of Service Using ATM over MPLS

An Asynchronous Transfer Mode (ATM) PW is used to carry ATM cells over an MPLS network. It is an evolutionary technology that allows you to migrate packet networks from legacy networks, yet provides transport for legacy applications. ATM over MPLS is particularly useful for transporting 3G voice traffic over MPLS networks.

You can configure ATM over MPLS in the following modes:

- N-to-1 Cell Mode—Maps one or more ATM virtual channel connections (VCCs) or virtual permanent connection (VPCs) to a single pseudowire.
- 1-to-1 Cell Mode—Maps a single ATM VCC or VPC to a single pseudowire.
- Port Mode—Map one physical port to a single pseudowire connection.

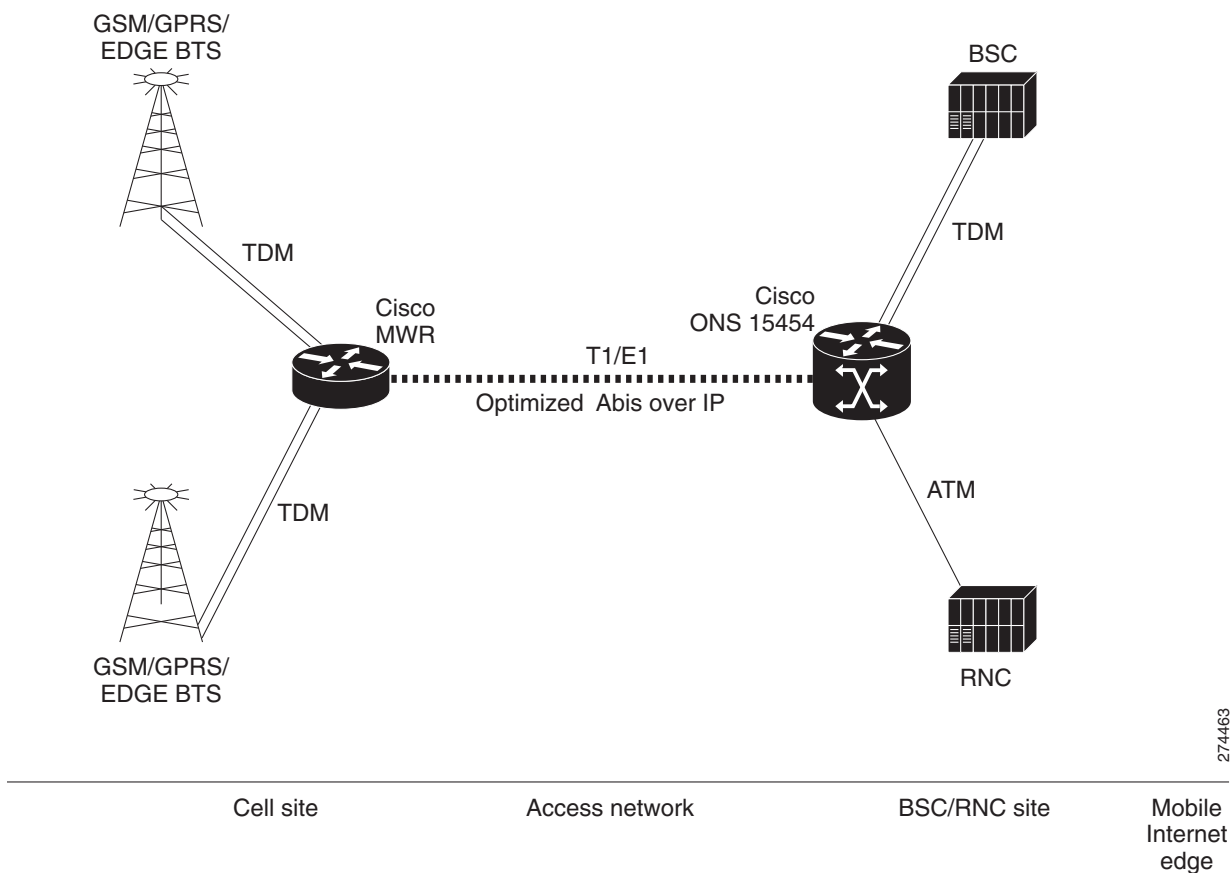
The Cisco MWR 2941-DC also supports cell packing and PVC mapping for ATM over MPLS pseudowires.

For more information about how to configure ATM over MPLS, see [“Configuring Transportation of Service Using ATM over MPLS” section on page 4-16](#). For sample ATM over MPLS configurations, see [“ATM over MPLS Configuration” section on page B-25](#).

## GSM Abis Optimization over IP Implementation

GSM Abis refers to the interface between the BTS and BSC in GSM system (the same term is used for CDMA systems). The Cisco MWR 2941-DC implementation of GSM Abis optimization over IP allows carriers to optimize voice and data traffic and maximize effective utilization of E1/T1 backhaul connections. [Figure 1-2](#) shows a Cisco MWR 2941-DC router in a network using GSM Abis Optimization over IP.

**Figure 1-2 Cisco MWR 2941-DC Router in a GSM Abis Optimization over IP—Example**



The Cisco GSM Abis optimization solution increases the T1/E1 bandwidth efficiency by as much as 50 percent:

1. Traffic loads can be carried using half as many T1/E1 trunks as previously used, allowing more voice and data calls to be carried over the existing RAN backhaul network.
2. The need to add new T1/E1 trunks is eliminated as traffic demands grow.
3. Existing trunks can be decommissioned (ending recurring costs).

Excess capacity is available in the existing RAN backhaul network. The operator can reallocate recovered bandwidth to carry traffic from other radios, such as GPRS, EDGE, 1xEV-DO, PWLANs, and other data overlays. The operator avoids costs of supplementing backhaul capacity. It also accelerates time to revenue from deployments of new radio technologies, as there is no need for the operator to be delayed until additional microwave licenses or leased-lines are supplied.

The Cisco MWR 2941-DC complies with 3GPP2 and 3GPP R5 and R6 transport standards. Cisco converts CDMA transport networks into 3 GPP2-compliant IP RAN transport networks, and GSM transport networks into R5/R6 IP RAN transport networks—and adds multiradio backhaul compression. Mobile wireless operators can leverage the benefits of IP transport in GSM RANs.

## Bidirectional Forwarding Detection

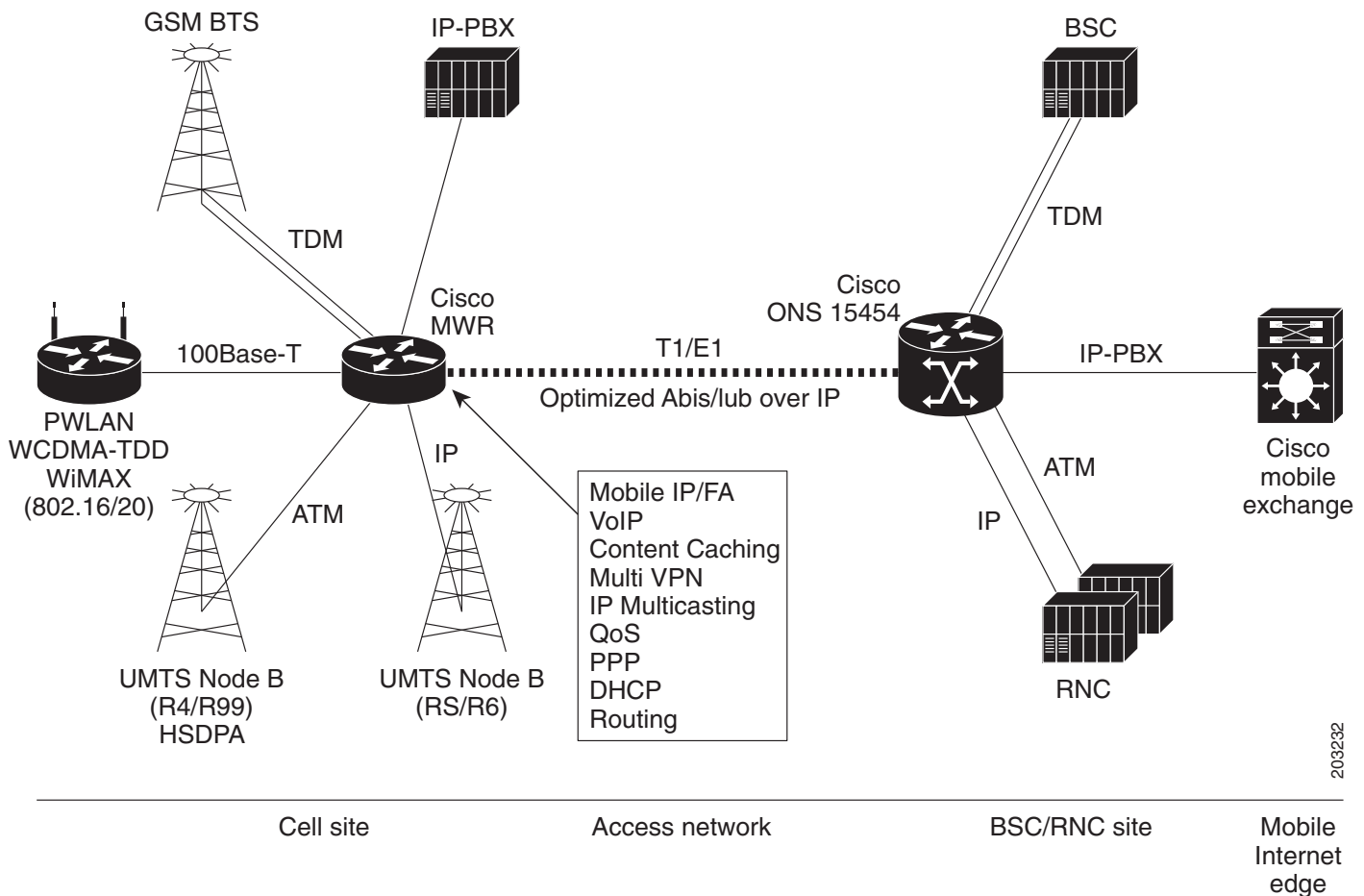
Bidirectional Forwarding Detection (BFD) provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. For instructions on how to configure BFD, see the [“Configuring BFD” section on page 4-39](#).

## Intelligent Cell Site IP Services

The Cisco RAN-O and IP-RAN solutions allow you to deliver profit-enhancing services. This is achieved through the set of IP networking features supported in Cisco IOS software that extends to the cell site (see [Figure 1-3 on page 1-6](#)).

## Cell Site Points-of-Presence

The cell site becomes a physical Point-of-Presence (POP) from which to offer hotspot services, or voice and wired ISP services, to nearby enterprises and residences. Because many cell sites are located in and around downtown areas, hotels, airports, and convention centers, they make attractive sites for co-locating public wireless LAN (PWLAN) access points and other wireless data overlays. Many of these wireless data radios are IP-based. IP networking features, like Mobile IP, VoIP, IP Multicast, VPN, and content caching, enable delivery of new revenue-generating services over these radios. The corresponding traffic “rides for free” on the spare backhaul bandwidth made available by Cisco Abis optimization solutions ([Figure 1-3](#)).

**Figure 1-3 Cisco MWR 2941-DC Router in a Cell Site POP—Example****Note**

The Cisco MWR 2941-DC router does not currently support UMTS Iub optimization.

## RAN-Optimization Implementation

In RAN-Optimization (RAN-O), the Cisco MWR 2941-DC router extends IP connectivity to the cell site and base transceiver station (BTS). The router provides bandwidth-efficient IP transport of GSM and UMTS voice and data bearer traffic, as well as maintenance, control, and signaling traffic, over the leased-line backhaul network between the BTS and leased-line termination and aggregation node through compression (cRTP/cUDP) and packet multiplexing (Multilink PPP).

## Cisco IOS Software Features

One version of the software is required for implementing the Cisco MWR 2941-DC router.



## Software Features

Standard Cisco IOS software features supported in the Cisco MWR 2941-DC router include:

### Simple Services

- DHCP
- PPP
- NAT
- OSPF
- RIP

### Intelligent Services

- QoS
- IP Multicast
- MPLS

### Additional Services

- ACFC and PFC handling during PPP negotiation
- SNMP
- NTP
- PTP and pseudowire-based timing
- TDM/PWE3 packet reordering

## Configuration Statements for CISCO-IP-RAN-BACKHAUL-MIB

This section describes how to enable notifications provided by the CISCO-IP-RAN-BACKHAUL-MIB.

In Cisco IOS Release 12.4(19)MR2, the Cisco MWR 2941-DC router supports the CISCO-IP-RAN-BACKHAUL-MIB.

This MIB is compatible with Cisco Mobile Wireless Transport Manager (MWTM) Version 5.0 or later, and provides information on the optimization of the following traffic types:

- GSM—Provides information between a Base Transceiver Station (BTS) and the corresponding Base Station Controller (BSC)
- UMTS—Provides information on optimization between a Node Band the corresponding Radio Network Controllers (RNC).

**Note**

The Cisco MWR 2941-DC does not currently support UMTS Iub optimization.

## Notifications

The notifications described in this section provide information on alarms, backhaul utilization, devices, and control generation. For more information on these notifications, see [Appendix A, “Cisco MWR 2941-DC Router Command Reference.”](#)

- **ciscoIpRanBackHaulGsmAlarm**

The **ciscoIpRanBackHaulGsmAlarm** notification provides information alarms associated with GSM-Abis interfaces. It only enables GSM Abis.

Example:

```
conf t
  snmp-server enable traps ipran alarm-gsm
```

- **ciscoIpRanBackHaulUmtsAlarm**

The **ciscoIpRanBackHaulUmtsAlarm** notification provides information alarms associated with UMTS-Iub interfaces. Only enables UMTS Iub.

Example:

```
conf t
  snmp-server enable traps ipran alarm-umts
```

- **ciscoIpRanBackHaulRcvdUtil + ciscoIpRanBackHaulSentUtil**

The **ciscoIpRanBackHaulRcvdUtil + ciscoIpRanBackHaulSentUtil** notification provides information on backhaul utilization. It only enables backhaul utilization.

Example:

```
conf t
  snmp-server enable traps ipran util
```



**Note** The **snmp-server enable traps ipran util** command is obsolete. Command line interface (CLI) accepts the command to maintain compatibility.

To specify all notifications, specify the component name.

Example:

```
conf t
  snmp-server enable traps ipran
```

The following commands (configuration statements) are used to provide additional information about device and control generation of notifications:

Command	Purpose
<b>ipran-mib backhaul-notify-interval</b>	Interval for backhaul utilization (Obsolete. Provided only to maintain compatibility.)
<b>ipran-mib location</b>	Location of device
<b>ipran-mib snmp-access</b>	Specify type SNMP connectivity
<b>ipran-mib threshold-acceptable</b>	Acceptable utilization threshold (Obsolete. Provided to maintain compatibility.)

Command	Purpose
<b>ipran-mib threshold-overloaded</b>	Overloaded utilization threshold (Obsolete. Provided to maintain compatibility.)
<b>ipran-mib threshold-warning</b>	Warning utilization threshold (Obsolete. Provided to maintain compatibility.)

# Network Management Features

This section provides an overview of the network management features for the Cisco MWR 2941-DC. For more information about management features on the Cisco MWR 2941-DC, see “[Monitoring and Managing the Cisco MWR 2941-DC Router](#)” section on page 4-46.

## Cisco Mobile Wireless Transport Manager (MWTM)

You can use Cisco network management applications, such as Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco MWR 2941-DC. This Network Management tool provides monitoring and management capabilities to the RAN-O solution. The Cisco MWTM addresses the element-management requirements of mobile operators and provides fault, configuration, and troubleshooting capability. For more information about MWTM, see [http://www.cisco.com/en/US/products/ps6472/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html).

## MIB Support

The Cisco MWR 2941-DC router supports the following MIBs:

<ul style="list-style-type: none"> <li>• CISCO-ACCESS-ENVMON-MIB</li> <li>• CISCO-CDP-MIB</li> <li>• CISCO-CONFIG-COPY-MIB</li> <li>• CISCO-CONFIG-MAN-MIB</li> <li>• CISCO-ENHANCED-MEMPOOL-MIB</li> <li>• CISCO-ENTITY-EXT-MIB</li> <li>• CISCO-ENTITY-FRU-CONTROL-MIB</li> <li>• CISCO-ENTITY-SENSOR-MIB</li> <li>• CISCO-ENTITY-VENDORTYPE-OID-MIB</li> <li>• CISCO-ENVMON-MIB</li> <li>• CISCO-FLASH-MIB</li> <li>• CISCO-IETF-PW-MIB</li> <li>• CISCO-IETF-PW-TC-MIB</li> <li>• CISCO-IF-EXTENSION-MIB</li> <li>• CISCO-IMAGE-MIB</li> <li>• CISCO-IP-RAN-BACKHAUL-MIB</li> <li>• CISCO-L2-TUNNEL-CONFIG-MIB</li> <li>• CISCO-MEMORY-POOL-MIB</li> <li>• CISCO-PROCESS-MIB</li> <li>• CISCO-PRODUCTS-MIB</li> <li>• CISCO-RTTMON-MIB</li> <li>• CISCO-SMI</li> <li>• CISCO-SYSLOG-MIB</li> </ul>	<ul style="list-style-type: none"> <li>• CISCO-TC</li> <li>• CISCO-VTP-MIB</li> <li>• ENTITY-MIB</li> <li>• HCNUM-TC</li> <li>• IANAifType-MIB</li> <li>• IF-MIB</li> <li>• IMA-MIB</li> <li>• INET-ADDRESS-MIB</li> <li>• MPLS-VPN-MIB</li> <li>• OLD-CISCO-CHASSIS-MIB</li> <li>• OLD-CISCO-INTERFACES-MIB</li> <li>• OLD-CISCO-SYS-MIB</li> <li>• OLD-CISCO-TS-MIB</li> <li>• PerfHist-TC-MIB</li> <li>• RMON2-MIB</li> <li>• RMON-MIB</li> <li>• SNMP-FRAMEWORK-MIB</li> <li>• SNMP-TARGET-MIB</li> <li>• SNMPv2-CONF</li> <li>• SNMPv2-MIB</li> <li>• SNMPv2-SMI</li> <li>• SNMPv2-TC</li> </ul>
--	---

## Limitations and Restrictions

The following limitations and restrictions apply to the Cisco MWR 2941-DC router.

### Hardware Limitations and Restrictions

The following hardware limitations and restrictions apply to the Cisco MWR 2941-DC router.

- The Cisco MWR 2941-DC router only supports the following HWICs:
  - HWIC-4T1/E1 (4 port clear-channel T1/E1 HWIC)

**Caution**

The Cisco MWR 2941-DC does not support online insertion and removal (OIR) of HWIC cards. Attempts to perform OIR on a card in a powered-on router might cause damage to the card.

## Software Limitations and Restrictions

The following software limitations and restrictions apply to the Cisco MWR 2941-DC router.

- UMTS Iub Optimization not supported—Release 12.4(19)MR2 does not support UMTS Iub Optimization.
- L2TP not supported—The MWR 2941 currently does not support L2TP.
- PTP Boundary mode not supported—This release does not support PTP Boundary mode.
- PTP Transparent mode not supported—This release does not support PTP Transparent mode.
- Channel group limitations on GSM-Abis interfaces—Only one channel group per E1/T1 is supported on GSM-Abis interfaces.
- Contiguous time slots on GSM-Abis channel groups—GSM-Abis channel groups cannot use non-contiguous time slots. For example, you can configure **channel-group 0 timeslot 8-20**, but not **channel-group 0 timeslot 1-5, 10-20**.
- Out-of-band master mode not supported—This release does not support out-of-band master mode for Timing over Packet/adaptive clock recovery. If your network design requires out-of-band master clocking, you can use the CEoPs SPA on the 7600 router for this purpose.
- ACR out-of-band payload limitation—The MWR 2941 only supports the payload-size values 486 (625 packets per second) or 243 (1250 packets per second) for out-of-band clock recovery.
- Limited OSPF support—Bidirectional Forwarding Detection (BFD) is supported on VLAN interfaces only. OSPF is the supported BFD client. When BFD and OSPF are used together with layer 2 redundancy applications such as Flexlink and a layer 2 network failure occurs, the Cisco MWR 2941-DC attempts to reestablish layer 2 redundancy. If the Cisco MWR 2941-DC cannot reestablish layer 2 redundancy before the defined BFD detection timeout, it attempts to re-establish BFD and OSPF redundancy using an alternate layer 3 path. If BFD detects a layer 3 failure while the Cisco MWR 2941-DC is attempting to reestablish layer 2 redundancy, increase the BFD timeout value.
- T1 SAToP is not supported on the HWIC-4T1/E1.
- L3VPNs (also known as MPLS VPNs) are not supported.

## New Features in Cisco IOS Release 12.4(19)MR2

The following features are supported in release 12.4(19)MR2 of the Cisco IOS software:

The following features are supported in release 12.4(19)MR2 of the Cisco IOS software:

- PWE3 Circuit Emulation over PSN (Packet Switched Network)—Allows you to create pseudowires (PWs) that emulate unstructured and structured T1s and E1s over an MPLS infrastructure, down to NxDS0 circuits. The Cisco MWR 2941-DC supports the following PWE3 standards:
  - Structure-agnostic TDM over Packet (SAToP)—Encapsulates TDM bit-streams (T1, E1, T3, E3) as PWs over PSNs; the feature is compliant with RFC 4553.

- Structure-aware TDM Circuit Emulation Service over Packet-Switched Network (CESoPSN)—Encapsulates structured (NxDS0) TDM signals as PWs over PSNs; the feature is compliant with RFC 5086.
  - Transportation of Service Using ATM over MPLS—Uses an Asynchronous Transfer Mode (ATM) PW to carry cells over an MPLS network; the feature is compliant with RFCs 4717 and 4816.
- GSM Abis Optimization over IP Implementation—Allows the Cisco MWR 2941-DC to optimize GSM voice and data traffic and maximize effective utilization of E1/T1 backhaul connections.
- Clocking features—Cisco IOS Release 12.4(19)MR2 introduces several new clocking features that are supported on the ASM-M2900-TOP daughter card, also known as the RTM Module. The RTM module supports the following new clocking features:
  - Precision Time Protocol (PTP)—Clocking and clock recovery based on the IEEE 1588-2008 standard; allows the Cisco MWR 2941-DC router to receive clocking from another PTP-enabled device or provide clocking to a PTP-enabled device.

This feature introduces a variety of new global commands: **ptp domain**, **ptp mode**, **ptp priority1**, and **ptp priority2**; the following interface commands: **ptp announce**, **ptp clock-destination**, **ptp clock-source**, **ptp delay-req**, **ptp enable**, **ptp master**, **ptp slave**, and **ptp sync**; and the following show commands: **show ptp clock**, **show ptp foreign-master-record**, **show ptp parent**, **show ptp port**, and **show ptp time-property**.

  - Adaptive Clock Recovery (ACR)—Also known as Timing over Packet (TOP), this feature allows the MWR 2941 to use in-band or out-of-band clocking on a virtual or regular TDM pseudowire interface. ACR allows the Cisco MWR 2941-DC to recover clocking from the headers of a packet stream and is compliant with the G.823 and G.824 standards. You can use the **recovered-clock slave** command to configure out-of-band clock recovery and the **recovered-clock recovered adaptive** command to configure adaptive clock recovery.
- Synchronous Ethernet—Allows the network to transport frequency and time information over Ethernet. You can use the **network-clock-select** command to configure synchronous Ethernet.



**Note** The RTM module is not required to use Synchronous Ethernet.

- ATM—This release includes ATM support with AAL0 and AAL5 encapsulation, F4 and F5 OAM (Operation, Administration, and Maintenance) monitoring, and Virtual Path (VP) shaping.
- IMA—This feature allows you to connect one or more interfaces to an ATM network using Inverse Multiplexing ATM (IMA). You can define IMA groups that can contain up to 8 bundles, with up to 24 links per bundle.
- IP Header Compression over PPP—This feature introduces support for IP header compression over PPP that is compliant with RFCs 2507, 2508, and 3544.
- Distributed Multilink PPP—Release 12.4(19)MR2 supports multilink PPP that is compliant with the RFC 1990 specification.
- Backup switch port interfaces using the **switchport backup interface** command.
- Flexlink
- IEEE 802.1d Ethernet Switching
- IEEE 802.1q VLANs
- VLAN Trunking Protocol (VTP)
- Per-VLAN Spanning Tree (PVST)+

- BITS Clocking
- Open Shortest Path First (OSPF)
- Bidirectional Forwarding Detection (BFD) for OSPF
- VPN Routing and Forwarding (VRF) Lite for OSPF
- ATM Cell Switching
- Label Distribution Protocol (LDP)





# CHAPTER 2

## Cisco IOS Software Basics

---

This chapter describes what you need to know about the Cisco IOS software before you configure the router by using the command-line interface (CLI). This chapter includes the following topics:

- [Getting Help](#), this page
- [Understanding Command Modes](#), page 2-1
- [Undoing a Command or Feature](#), page 2-2
- [Saving Configuration Changes](#), page 2-3

Understanding this information saves you time as you use the CLI. If you have never used the Cisco IOS software or if you need a review, read this chapter before you proceed to [Chapter 3, “First-Time Configuration.”](#)

If you are already familiar with the Cisco IOS software, go to [Chapter 3, “First-Time Configuration.”](#)

### Getting Help

Use the question mark (?) and arrow keys to help you enter commands:

- For a list of available commands, enter a question mark:

```
Router> ?
```

- To complete a command, enter a few known characters followed by a question mark (with no space):

```
Router> s?
```

- For a list of command variables, enter the command followed by a space and a question mark:

```
Router> show ?
```

- To redisplay a command that you previously entered, press the **Up Arrow** key. Continue to press the **Up Arrow** key to see more commands.

### Understanding Command Modes

The Cisco IOS user interface is used in various command modes. Each command mode permits you to configure different components on your router. The commands available at any given time depend on which command mode you are in. Entering a question mark (?) at a prompt displays a list of commands available for that command mode. The following table lists the most common command modes.

Command Mode	Access Method	Router Prompt Displayed	Exit Method
User EXEC	Log in.	Router>	Use the <b>logout</b> command.
Privileged EXEC	From user EXEC mode, enter the <b>enable</b> command.	Router#	To exit to user EXEC mode, use the <b>disable</b> , <b>exit</b> , or <b>logout</b> command.
Global configuration	From the privileged EXEC mode, enter the <b>configure terminal</b> command.	Router (config)#	To exit to privileged EXEC mode, use the <b>exit</b> or <b>end</b> command, or press <b>Ctrl-Z</b> .
Interface configuration	From the global configuration mode, enter the <b>interface type number</b> command, such as <b>interface serial 0/0</b> .	Router (config-if)#	To exit to global configuration mode, use the <b>exit</b> command.  To exit directly to privileged EXEC mode, press <b>Ctrl-Z</b> .

**Timesaver**

Each command mode restricts you to a subset of commands. If you have trouble entering a command, check the prompt and enter the question mark (?) to see a list of available commands. You might be in the incorrect command mode or be using an incorrect syntax.

In the following example, notice how the prompt changes after each command to indicate a new command mode:

```
Router> enable
Password: <enable password>
Router# configure terminal
Router (config)# interface serial 0/0
Router (config-if)# line 0
Router (config-line)# controller t1 0
Router (config-controller)# exit
Router (config)# exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

The last message is normal and does not indicate an error. Press **Return** to get the Router# prompt.

**Note**

You can press **Ctrl-Z** in any mode to immediately return to enable mode (Router#), instead of entering **exit**, which returns you to the previous mode.

## Undoing a Command or Feature

If you want to undo a command that you entered or if you want to disable a feature, enter the keyword **no** before most commands; for example, **no ip routing**.

# Saving Configuration Changes

To save your configuration changes to NVRAM, so that the changes are not lost during a system reload or power outage, enter the **copy running-config startup-config** command. For example:

```
Router# copy running-config startup-config  
Building configuration...
```

It might take a few minutes to save the configuration to NVRAM. After the configuration has been saved, the following message appears:

```
[OK]  
Router#
```





# CHAPTER 3

## First-Time Configuration

---

This chapter describes the actions to take before turning on your router for the first time. This chapter includes the following sections:

- [Understanding the Cisco MWR 2941-DC Router Interface Numbering, page 3-1](#)
- [Setup Command Facility, page 3-3](#)
- [Configuring Global Parameters, page 3-3](#)
- [Completing the Configuration, page 3-6](#)

## Understanding the Cisco MWR 2941-DC Router Interface Numbering

Each network interface on a Cisco MWR 2941-DC router is identified by a slot number and a port number.

[Figure 3-1 on page 3-2](#) shows an example of interface numbering on a Cisco MWR 2941-DC router:

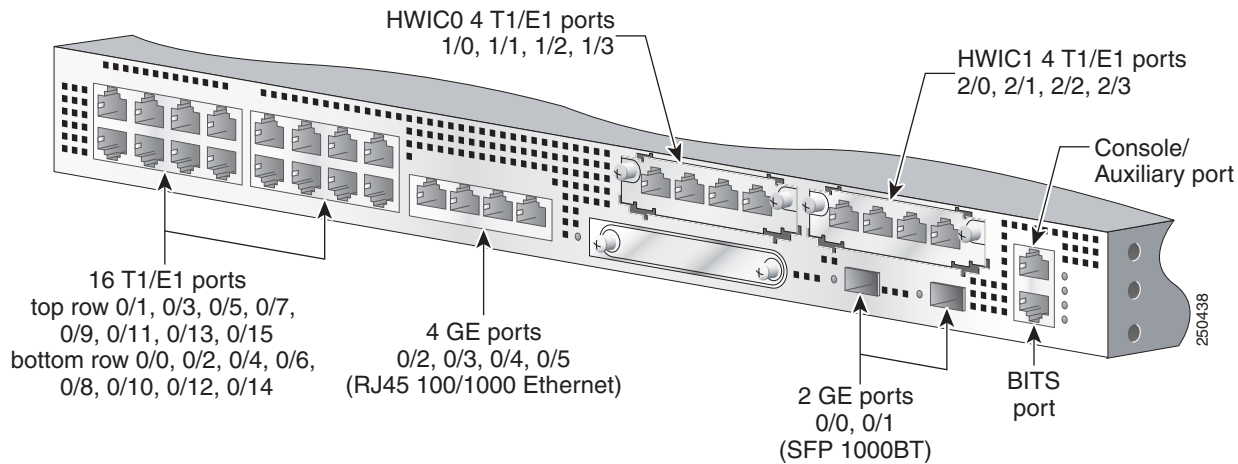
- A Cisco HWIC-4T1/E1 interface card in both HWIC slots
- Two built-in Gigabit Ethernet small form-factor pluggable (SFP) interfaces (labeled GE0 and GE1)
- Four built-in Gigabit Ethernet interfaces (labeled L2–L5)
- 16 E1/T1 ports (labeled C1AL–C15AL)



### Note

The two HWIC cards shown in [Figure 3-1](#) are not included with the Cisco MWR 2941-DC router; you must order them separately.

---

**Figure 3-1 Cisco MWR 2941-DC Router Port Numbers**

## Slot and Port Numbering

The Cisco MWR 2941-DC router chassis contains the following interface types:

- 16 T1/E1 ports, labeled “T1/E1”
- 4 RJ-45 jacks for copper Ethernet ports, labeled “100/1000” Ethernet
- 2 HWIC slots, labeled “HWIC0” and “HWIC1”
- 1 compact FLASH Type-II connector, labeled “Compact Flash”
- 2 SFP connectors for optical GE ports, labeled “GE0” and “GE1”
- 1 RJ-45 connector for Console/Auxiliary, labeled “CON/AUX”
- 1 RJ-45 jack for BITS interface, labeled “BITS”

The logical slot numbers are 0 for all built-in interfaces.

The numbering format is:

Interface type Slot number/Interface number

Interface (port) numbers begin at logical 0 for each interface type.

Following is an explanation of the slot/port numbering:

- Logical interface numbering for the built-in T1/E1 ports runs from 0/0 through 0/15. Interfaces are hardwired; therefore, port 0 is always logical interface 0/0, port 1 is always logical interface 0/1, and so on. Built-in T1/E1 ports are numbered bottom to top, left to right (bottom row numbered 0-2-4-6-8-10-12-14, top row numbered 1-3-5-7-9-11-13-15).
- When the 2 HWIC slots are used to expand the T1/E1 port density to 20 or 24 ports, logical interface numbering continues from 1/0 through 1/3 and 2/0 through 2/3. Logical interfaces for HWIC0 are always 1/0 through 1/3 and logical interfaces for HWIC1 are always 2/0 through 2/3. Because the interfaces are hardwired, HWIC0 port 0 is always logical interface 1/0, HWIC0 port 1 is always logical interface 1/1, HWIC1 port 0 is always logical interface 2/0, HWIC1 port 1 is always logical interface 2/1, and so on. Ports are numbered left to right for each HWIC.

Logical interface numbering for the built-in Ethernet ports runs from 0/0 through 0/5. Because the interfaces are hardwired, port 0 is always logical interface 0/0, port 1 is always logical interface 0/1, and so on. SFP ports are numbered left to right, 0 and 1; 100/1000 Ethernet ports are numbered left to right, 2 through 5.

## Setup Command Facility

The **setup** command facility prompts you for information that is required to start a router functioning quickly. The facility steps you through a basic configuration, including LAN interfaces.

If you prefer to configure the router manually or to configure a module or interface that is not included in the **setup** command facility, go to [“Chapter 2, “Cisco IOS Software Basics”](#) to familiarize yourself with the command-line interface (CLI). Then, go to [Chapter 4, “Configuring the Cisco MWR 2941-DC Router Using the CLI.”](#)

## Before Starting Your Router

Before you power on your router and begin using the **setup** command facility, follow these steps:

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Set up the hardware and connect the console and network cables as described in the “Connecting Cables” section of the <i>Cisco MWR 2941-DC Router Hardware Installation Guide</i> . |
| <b>Step 2</b> | Configure your PC terminal emulation program for 9600 baud, 8 data bits, no parity, and 1 stop bit.   |
- 

## Using the Setup Command Facility

The **setup** command facility appears in your PC terminal emulation program window.

To create a basic configuration for your router, do the following:

- Complete the steps in the [“Configuring Global Parameters”](#) section on page 3-3
- Complete the steps in the [“Completing the Configuration”](#) section on page 3-6



---

**Note** If you make a mistake while using the setup command facility, you can exit the facility and run it again. Press **Ctrl-C**, and type **setup** at the enable mode prompt (1900#).

---

## Configuring Global Parameters

Use the following procedure to configure global parameters.

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Power on the router. Messages appear in the terminal emulation program window. |
|---------------|--|
-

**Caution**

*Do not press any keys on the keyboard until the messages stop. Any keys that you press during this time are interpreted as the first command entered after the messages stop, which might cause the router to power off and start over. Wait a few minutes. The messages stop automatically.*

The messages look similar to the following:

**Note**

The messages vary, depending on the Cisco IOS software image and interface modules in your router. This section is for reference only, and output might not match the messages on your console.

```
rommon 1 >boot
program load complete, entry point:0x80008000, size:0xc200

Initializing ATA monitor library.....
program load complete, entry point:0x80008000, size:0xc200

Initializing ATA monitor library.....
program load complete, entry point:0x80008000, size:0xc35eec
Self decompressing the image:
#####
#####
#####
#####
#####
#####
#####
#####
##### [OK]

Smart Init is enabled
smart init is sizing iomem
      ID  MEMORY_REQTYPE
0035C  0X005F3C00 MWR2941 Mainboard
        0X000F3BB0 public buffer pools
        0X00843000 public particle pools
TOTAL: 0X06894CB0

If any of the above Memory requirements are "UNKNOWN", you may be using an
unsupported configuration or there is a software problem and system operation
may be compromised.
Rounded IOMEM up to: 104Mb.
Using 20 percent iomem. [104Mb/512Mb]
```

#### Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, California 95134-1706

Cisco IOS Software, 2900 Software (MWR2900-IPRAN-M),  
Experimental Version 12.4(20050412:070057),  
Copyright (c) 1986-2009 by Cisco Systems, Inc.



```

Compiled Sat 10-Jan-09 03:19 by cbrezove
Image text-base:0x60008F60, data-base:0x6106A000

Cisco Systems, Inc. MWR-2941-DC (MPC8347E) processor (revision 0x400) with 41719
6K/107092K bytes of memory.
Processor board ID
MPC8347E CPU Rev: Part Number 0x8032, Revision ID 0x300
1 RTM Module: ASM-M2900-TOP daughter card
6 Gigabit Ethernet interfaces
1 terminal line
128K bytes of non-volatile configuration memory.
125440K bytes of ATA CompactFlash (Read/Write)

--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

```

**Step 2** To begin the initial configuration dialog, enter **yes** when the following message appears:

```

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

```

```

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

```

**Step 3** Enter a hostname for the router (this example uses 2941-1).

```

Configuring global parameters:

```

```

Enter host name [Router]: 2941-1

```

**Step 4** Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration.

```

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: ciscoenable

```



**Note** When you enter the enable secret password, the password is visible while you type the it. After you enter the password, it becomes encrypted in the configuration.

**Step 5** Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration.

```

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: ciscoenable

```

**Step 6** To prevent unauthenticated access to the router through ports other than the console port, enter the virtual terminal password.

```

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: ciscoterminal

```

**Step 7** Respond to the following prompts as appropriate for your network:

```
Configure SNMP Network Management? [yes]:
Community string [public]: public
```

- Step 8** The summary of interfaces appears. This list varies, depending on the network modules installed in your router.

```
Current interface summary
```

```
Any interface listed with OK? value "NO" does not have a valid configuration
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	NO	unset	up	up
GigabitEthernet0/1	unassigned	NO	unset	up	up

- Step 9** Specify the interface to be used to connect to the network management system.

```
Enter interface name used to connect to the
management network from the above interface summary: GigabitEthernet0/0
```

- Step 10** Configure the specified interface as prompted.

```
Configuring interface GigabitEthernet0/0:
Configure IP on this interface? [no]:
```

## Completing the Configuration

When you have provided all of the information prompted for by the setup command facility, the configuration appears. Messages similar to the following appear:

The following configuration command script was created:

```
!
hostname 2941-1
enable secret 5 $1$5fH0$Z6Pr5EgtR5iNJ2nBg3i6y1 enable password ciscoenable line vty 0 4
password ciscoenablesnmp-server community public !
no ip routing

!
interface GigabitEthernet0/0
media-type 100BaseX
full-duplex
ip address 178.18.44.233 255.255.255.128
!
interface GigabitEthernet0/1
shutdown
no ip address
!
end
```

To complete your router configuration, do the following:

- Step 1** A setup command facility prompt you to save this configuration.

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

```
Enter your selection [2]: 2
Building configuration...
```

[OK]

Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!

If you answer:

- **no**—The configuration information that you entered is *not* saved, and you return to the router enable prompt. To return to the system configuration dialog, enter **setup**.
- **yes**—The configuration is saved, and you return to the EXEC prompt.

**Step 2** When the messages stop displaying in your window, press **Return** to view the command line prompt.

---

The 2941-1> prompt indicates that you are now at the CLI and you have just completed a basic router configuration. However, this is *not* a complete configuration. You must configure additional parameters by using the Cisco IOS software CLI as described in [Chapter 4, “Configuring the Cisco MWR 2941-DC Router Using the CLI.”](#)





## CHAPTER 4

# Configuring the Cisco MWR 2941-DC Router Using the CLI

---

This chapter describes how to use the Cisco IOS software command-line interface (CLI) to configure the Cisco MWR 2941-DC Mobile Wireless Edge Router in a RAN-O solution and includes the following sections:

- [Verifying the Cisco IOS Software Version, page 4-1](#)
- [Configuration Sequence, page 4-1](#)
- [Monitoring and Managing the Cisco MWR 2941-DC Router, page 4-46](#)

For sample configurations, see [Appendix B, “Configuration Examples.”](#)

For additional configuration topics, see the Cisco IOS configuration guide and command reference publications. These publications are available on the Documentation DVD that shipped with your router, available online at Cisco.com, or as printed copies that you can order separately.



### Note

If you skipped [Chapter 2, “Cisco IOS Software Basics,”](#) and you have never configured a Cisco router, return to Chapter 2 and read it now. The chapter contains important information that you need to successfully configure your router.

---

## Verifying the Cisco IOS Software Version

To implement the Cisco MWR 2941-DC router in a RAN-O solution, Cisco IOS Release 12.4(19)MR2 or 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 the configuration files, and the boot images.

## Configuration Sequence

The [Summary of Steps](#) section provides the recommended primary configuration sequence for the Cisco MWR 2941-DC router in a RAN-O solution. These steps have configuration substeps (or tasks) within the primary steps or tasks.

**Note**

The installation of the Cisco MWR 2941-DC router and the Cisco T1/E1 interface card should be completed before attempting the configuration (see the [“Related Documentation”](#) section on page ix for more information).

The configuration sequence of the Cisco MWR 2941-DC router for the RAN-O solution assumes that you will have already had some familiarity with the configuration of Cisco routers. It is also assumed that you are familiar with your own network configurations and that you are familiar with the Command Line Interface (CLI) used in configuring Cisco routers.

**Note**

For correct CLI syntax and format, see the [“Cisco MWR 2941-DC Router Command Reference”](#) section on page A-1.

## Summary of Steps

To configure the Cisco MWR 2941-DC router in a RAN-O solution, perform the following tasks.

1. [Configuring the Hostname and Password](#)
2. [Verifying the Hostname and Password, page 4-3](#)
3. [Configuring Gigabit Ethernet Interfaces, page 4-4](#)
4. [Configuring Network Clocking Support, page 4-6](#)
5. [Configuring Pseudowire, page 4-13](#)
6. [Configuring MLPPP Backhaul, page 4-22](#)
7. [Configuring GSM-Abis Links, page 4-31](#)
8. [Configuring SNMP Support, page 4-33](#)
9. [Configuring ATM IMA, page 4-37](#)
10. [Configuring Satellite Support in a RAN-O Network, page 4-40](#)
11. [Configuring Graceful Degradation, page 4-42](#)
12. [Saving Configuration Changes, page 4-45](#)

## Configuring the Hostname and Password

First configure the hostname and set an encrypted password. Configuring a hostname allows you to distinguish multiple Cisco routers from each other. Setting an encrypted password allows you to prevent unauthorized configuration changes.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the Router# prompt.

To configure a hostname and to set an encrypted password, follow these steps:

**Step 1** Enter enable mode.

```
Router> enable
```

The Password prompt appears. Enter your password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

- Step 2** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

When the prompt changes to `Router(config)`, you have entered global configuration mode.

```
Router(config)#
```

- Step 3** Change the name of the router to a meaningful name. Substitute your hostname for `Router`.

```
Router(config)# hostname Router
```

```
Router(config)#
```

- Step 4** Enter an enable secret password. This password provides access to privileged EXEC mode. When you type **enable** at the EXEC prompt (`Router>`), you must enter the enable secret password to access configuration mode. Enter your secret password.

```
Router(config)# enable secret secret password
```

- Step 5** Exit back to global configuration mode.

```
Router(config)# exit
```

---

## Verifying the Hostname and Password

To verify that you have correctly configured the hostname and password, follow these steps

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

```
Router# show config  
Using 1888 out of 126968 bytes  
!  
version XX.X  
.  
.  
.  
!  
hostname Router  
!  
enable secret 5 $1$60L4$X2JY0woDc0.kqa1loO/w8/  
.  
.  
.
```

- Step 2** Check the hostname and encrypted password, which appear near the top of the command output.

- Step 3** 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: password
Router#
```

---

## Configuring Gigabit Ethernet Interfaces

To configure the Gigabit Ethernet (GE) interface on the Cisco MWR 2941-DC, complete the following tasks:

- [Configuring the GE Interface Properties, page 4-4](#)
- [Setting the Speed and Duplex Mode, page 4-5](#)
- [Enabling the GE Interface, page 4-5](#)
- [Creating Backup Switch Interfaces, page 4-6](#)

### Configuring the GE Interface Properties

Perform a basic Gigabit Ethernet IP Address configuration by specifying the port adapter and aligning an IP address and subnet mask of the interface as follows.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the **Router#** prompt.

**Note**

The spanning tree-related commands described in this section are optional.

To configure the GE interface, follow these steps while in global configuration mode:

- 
- Step 1** Specify the port adapter type and the location of the interface to be configured.

```
Router(config)# interface gigabitethernet slot/port
Router(config-if)#
```

The *slot* is always 0 and the *port* is the number of the port (0 or 1).

- Step 2** To set the interface type, use the **switchport mode** command.

```
Router(config-if)# switchport mode {access | trunk}
```

- Step 3** To prioritize an interface when two bridges compete for position as the root bridge, use the **spanning tree port-priority** command.

```
Router(config-if)# spanning-tree port-priority port_priority
```

- Step 4** To calculate the path cost of STP on an interface, use the **spanning-tree cost** command.

```
Router(config-if)# spanning-tree cost port_cost
```

- Step 5** For interfaces that connect to end stations, you can use the **spanning-tree portfast** command to set the interface to move directly to the spanning-tree forwarding state when linkup occurs.

```
Router(config-if)# spanning-tree portfast
```



**Step 6** To enable Cisco Discovery Protocol (CDP) on the router, use the **cdp enable** command.

```
Router(config-if)# cdp enable
```

---

## Setting the Speed and Duplex Mode

The Gigabit Ethernet ports of the Cisco MWR 2941-DC router can run in full or half- duplex mode—100 Mbps or 1000 Mbps (1 Gbps). The Cisco MWR 2941-DC router has an autonegotiation feature that allows the router to negotiate the speed and duplex mode with the corresponding interface at the other end of the connection.

Autonegotiation is the default setting for the speed and transmission mode.

When you configure an interface speed and duplex mode, follow these guidelines:

- If both ends of the line support autonegotiation, we highly recommend the use of default autonegotiation settings.
- When autonegotiation is turned on for either speed or duplex mode, it autonegotiates both speed and the duplex mode.
- If one interface supports autonegotiation, and the interface at the other end does not, configure the duplex mode and speed on both interfaces. If you use the autonegotiation setting on the supported side, the duplex mode setting is set at half-duplex.



**Note** In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

---

To configure speed and duplex operation, follow these steps while in interface configuration mode:

**Step 1** Specify the duplex operation.

```
Router(config-if)# duplex [auto | half | full]
```

**Step 2** Specify the speed.

```
Router(config-if)# speed [auto | 1000 | 100]
```

---

## Enabling the GE Interface



**Note** In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

---

After you configure the GE interface, enable it using the `no shutdown` command by following this step

```
Router(config-if)# no shutdown
```

## Creating Backup Switch Interfaces

You can use the following command to create a backup switch interface:

```
Rounders(conf-if)# switchport backup interface interface_name preemption [forced | bandwidth | off] delay [time]
```

For more information about this command, see [switchport backup interface](#), page A-120

## Configuring VLANs

The Cisco MWR 2941-DC router supports a full set of VLAN features. For instructions on how to configure VLANs, see the Cisco IOS LAN Switching Configuration Guide, Release 12.4T at [http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/12\\_4t/lsw\\_12\\_4t\\_book.html](http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/12_4t/lsw_12_4t_book.html).

## Configuring Network Clocking Support

This section describes the network clocking support on the Cisco MWR 2941-DC router.

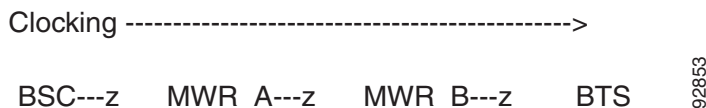
## Network Clocking Overview

Network clocking is:

- The means by which a clock signal is generated or derived and distributed through a network and its individual nodes for the purpose of ensuring synchronized network operation.
- An important consideration in the RAN-O networks. Solid network clocking design helps the successful deployment of any RAN-O network.

Figure 4-1 shows an example of network clocking on a RAN-O network using the Cisco MWR 2941-DC.

**Figure 4-1      Clocking Example**



The base station controller (BSC) provides the clock source:

- Into the network to which the connected devices must synchronize its transmit clocks.
- To the Cisco MWR 2941-DC router, which is distributed to the participating serial and ATM ports.

## Network Clocking on the Cisco MWR 2941-DC

The Cisco MWR 2941-DC supports multiple types of network clocking:

- **Precision Time Protocol (PTP)**—Clocking and clock recovery based on the IEEE 1588-2008 standard; allows the Cisco MWR 2941-DC router to receive clocking from another PTP-enabled device or provide clocking to a PTP-enabled device. To configure PTP clocking, see [Configuring PTP Clocking](#).

- Pseudowire-based clocking—Allows the Cisco MWR 2941-DC router to use clocking using a pseudowire or virtual pseudowire interface. Pseudowire-based clocking supports adaptive clock recovery, which allows the Cisco MWR 2941-DC to recover clocking from the headers of a packet stream. To configure pseudowire-based clocking, see [Configuring Pseudowire-based Clocking with Adaptive Clock Recovery](#)
- Synchronous Ethernet—Allows the network to transport frequency and time information over Ethernet. To configure synchronous Ethernet, use the **network-clock-select** command described in the [Configure the Global Network Clock](#) section.

**Note**

The Cisco MWR 2941-DC does not support the use of PTP and PWE-based clocking at the same time.

## Configuring PTP Clocking

This section describes how to configure PTP-based clocking on the Cisco MWR 2941-DC. For more information about the PTP commands, see, [Appendix A, “Cisco MWR 2941-DC Router Command Reference.”](#)

**Note**

The settings shown in this section are an example only; you must determine the appropriate PTP settings based upon your network clocking design.

## Configuring Global PTP Settings

**Step 1**

Enter the following commands to configure the global PTP settings:

- a. Use the **PTP mode** command to specify the PTP mode.

```
Router(config)# ptp mode ordinary
```

- b. Use the **PTP priority1** command to configure the preference level for a clock; slave devices use the priority1 value when selecting a master clock.

```
Router(config)# ptp priority1 128
```

- c. Use the **PTP priority2** command to set a secondary preference level for a clock; slave devices use the priority2 value when selecting a master clock.

```
Router(config)# ptp priority2 128
```

- d. Use the **PTP domain** command to specify the PTP domain number that the router uses. PTP domains allow you to use multiple independent PTP clocking subdomains on a single network.

```
Router(config)# ptp domain 6
```

## Configuring the PTP Mode

Table 4-1 summarizes the PTP mode commands that you can use on the Cisco MWR 2941-DC.

**Table 4-1 PTP Mode Commands**

Command	Purpose
ptp announce	Sets interval and timeout values for PTP announcement packets.
ptp sync	Specifies the interval that the router uses to send PTP synchronization messages.
ptp delay-req interval	Specifies the delay request interval, the time recommended to member devices to send delay request messages when an interface is in PTP master mode.
ptp clock-source	Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode.
ptp clock-destination	Specifies the IP address of a clock destination. This command only applies when the router is in PTP master unicast mode.
ptp enable	Enables PTP mode on an interface

The following examples demonstrate how to use these commands to configure each of the six PTP modes. Use the appropriate section based on the PTP mode that you want to configure on the Cisco MWR 2941-DC.

- PTP multicast master mode—Sets the Cisco MWR 2941-DC to act as the master PTP clock. Multicast specifies that the router sends PTP messages to all the slaves listening on the PTP multicast group.

```
Router(config)# interface Vlan10
Router(config-if)# ip address 172.18.52.38 255.255.255.0
Router(config-if)# ip igmp join-group 224.0.1.129
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp master multicast
Router(config-if)# ptp enable
```

- PTP multicast slave mode—Sets the Cisco MWR 2941-DC to receive clocking from a PTP master device in multicast mode.

```
Router(config)# interface Vlan10
Router(config-if)# ip address 172.18.52.38 255.255.255.0
Router(config-if)# ip igmp join-group 224.0.1.129
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave multicast
Router(config-if)# ptp enable
```

- PTP unicast master mode—Sets the Cisco MWR 2941-DC to act as the master PTP clock. Unicast specifies that the router sends PTP messages to a single slave host.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 172.18.52.38 255.255.255.0
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp master unicast
```

```
Router(config-if)# ptp clock-destination 172.18.52.201
Router(config-if)# ptp enable
```

- PTP unicast slave mode—Sets the Cisco MWR 2941-DC to receive clocking from a single PTP master device.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 172.18.52.38 255.255.255.0
Router(config-if)# ptp announce interval 3
Router(config-if)# ptp announce timeout 2
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave unicast
Router(config-if)# ptp clock-source 172.18.52.10
Router(config-if)# ptp enable
```

- PTP unicast master mode (with negotiation enabled)—Sets the Cisco MWR 2941-DC to send clocking to a single PTP slave device; the router allows the slave devices to negotiate their master clock device.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 172.18.52.38 255.255.255.0
Router(config-if)# ptp announce interval 0
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp master unicast negotiation
Router(config-if)# ptp clock-destination 172.18.52.201
Router(config-if)# ptp enable
```

- PTP unicast slave mode (with negotiation enabled)—Sets the Cisco MWR 2941-DC to receive clocking from a PTP master devices; the router negotiates between up to 128 PTP master devices.

```
Router(config)# interface Vlan2
Router(config-if)# ip address 172.18.52.38 255.255.255.0
Router(config-if)# ptp announce interval 3
Router(config-if)# ptp announce timeout 2
Router(config-if)# ptp sync interval -6
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp slave unicast negotiation
Router(config-if)# ptp clock-source 172.18.52.10
Router(config-if)# ptp enable
```

**Note**

You can only configure one VLAN interface for PTP.

## Configure the Global Network Clock

Use the **network-clock-select** command to configure clock selection for the entire network.

- If you configured the router for PTP master mode, set one or more external clock sources using the **network-clock-select** command with the synchronous ethernet (sync), bits, or E1 or T1 interface parameters:

```
Router(config)# network-clock-select 1 BITS
Router(config)# network-clock-select 2 SYNC 0
Router(config)# network-clock-select 3 E1 0/0
```

- If you configured the router for PTP slave mode, enter the following commands:

```
Router(config)# network-clock-select 1 PACKET-TIMING
Router(config)# network-clock-select hold-timeout 900
```

For more information about the **network-clock-select** command, see [Appendix A, “Cisco MWR 2941-DC Router Command Reference.”](#)

**Note**

The minimum network-clock-select hold-timeout value recommended in the slave mode is 900 seconds or 15 minutes.

## Configuring Pseudowire-based Clocking with Adaptive Clock Recovery

Follow these steps to configure pseudowire-based clocking with adaptive clock recovery:

The Cisco MWR 2941-DC supports the following adaptive clock recovery modes:

- In-band master mode—The Cisco MWR 2941-DC provides clocking to slave devices using the headers in a packet stream. To configure this clocking mode, see [Configuring In-Band Master Mode](#).
- In-band slave mode—The Cisco MWR 2941-DC receives clocking from a master clock using the headers from a packet stream. To configure this clocking mode, see [Configuring In-Band Slave Mode](#).
- Out-of-band slave mode—The Cisco MWR 2941-DC receives clocking from a master clock using dedicated packets for timing. To configure this clocking mode, see [Configuring Out-of-Band Slave Mode](#).

**Note**

The Cisco MWR 2941-DC currently does not support out-of-band master mode.

### Configuring In-Band Master Mode

- Step 1** To configure in-band ACR master mode, you must configure Structure-agnostic TDM over Packet (SAToP) or Circuit Emulation Service (CES).

- The following example shows how to configure SAToP.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 0 unframed
```

- The following example shows how to configure CES.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 3 timeslots 1-31
```

- Step 2** Configure the loopback interface.

```
Router(config)# interface Loopback
Router(config-if)# ip address 10.88.88.99 255.255.255.255
```

- Step 3** Configure the VLAN interface.

```
Router(config)# interface Vlan1
Router(config-if)# ip address 172.18.52.2 255.255.255.0
Router(config-if)# no ptp enable
Router(config-if)# mpls ip
```

- Step 4** Configure MPLS.

```
Router(config)# mpls ldp router-id Loopback0 force
```

**Step 5** Configure the CEM interface.

```
Router(config)# interface cem 0/1
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.2 7600 encaps mpls
```

**Step 6** Set one or more external clock sources using the synce, bits, or E1 interface, or T1 interface parameters:

```
Router(config)# network-clock-select 1 BITS
```

## Configuring In-Band Slave Mode

**Step 1** To configure in-band ACR slave mode, you must configure Structure-agnostic TDM over Packet (SAToP) or Circuit Emulation Service (CES).

- The following example shows how to configure SAToP.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 0 unframed
```

- The following example shows how to configure CES.

```
Router(config)# controller e1 0/0
Router(config-controller)# clock source internal
Router(config-controller)# cem-group 3 timeslots 1-31
```

**Step 2** Enter the following commands to configure the loopback interface.

```
Router(config)# interface Loopback
Router(config-if)# ip address 10.88.88.99 255.255.255.255
```

**Step 3** Enter the following commands to configure the VLAN interface.

```
Router(config)# interface Vlan1
Router(config-if)# ip address 172.18.52.10.2 255.255.255.0
Router(config-if)# no ptp enable
Router(config-if)# mpls ip
```

**Step 4** Enter the following command to configure MPLS.

```
Router(config)# mpls ldp router-id Loopback0 force
```

**Step 5** Enter the following commands to configure the CEM interface.

```
Router(config)# interface cem 0/1
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.2 7600 encaps mpls
```

**Step 6** Enter the following command to configure adaptive clock recovery using a circuit emulation (CEM) interface:

```
Router(config)# recovered-clock recovered adaptive cem 0 0 1
```

**Step 7** Enter the following commands to configure the network clock:

```
Router(config)# network-clock-select 1 PACKET-TIMING
Router(config)# network-clock-select hold-timeout 900
```

## Configuring Out-of-Band Slave Mode



**Note** When configuring out-of-band clocking, verify that the edge router (such as the Cisco 7600 Series Router) has the same out-of-band clocking settings.

**Step 1** Enter the following command to configure clock recovery in slave mode:

```
Router(config)# recovered-clock slave
```

**Step 2** Enter the following commands to configure the loopback interface.

```
Router(config)# interface Loopback  
Router(config-if)# ip address 10.88.88.99 255.255.255.255
```

**Step 3** Enter the following commands to configure the VLAN interface.

```
Router(config)# interface Vlan1  
Router(config-if)# ip address 172.18.52.10.2 255.255.255.0  
Router(config-if)# no ptp enable  
Router(config-if)# mpls ip
```

**Step 4** Enter the following command to configure MPLS.

**Step 5** Router(config)# **mpls ldp router-id Loopback0 force**

**Step 6** Enter the following commands to configure the CEM interface:

```
Router(config)# interface virtual-cem 0/24  
Router(config-if)# payload-size 486  
Router(config-if)# cem 0  
Router(config-if-cem)# xconnect 10.10.10.2 7600 encaps mpls
```



**Note** The Cisco MWR 2941-DC only supports a payload size of 486 (625 packets per second) or 243 (1250 packets per second). This value affects the payload size only and does not alter the packet size, which is constant regardless of payload value.

**Step 7** Enter the following commands to configure the network clock:

```
Router(config)# network-clock-select 1 PACKET-TIMING  
Router(config)# network-clock-select hold-timeout 900
```

## Verifying Clock-related Settings

Use the following commands to verify the clock settings

- **show network-clocks**—Displays information about the network clocks
- **show controller**—Displays the status of the controller, including clocking information.
- **show ptp clock**—Displays ptp clock information
- **show ptp foreign-master-record**—Displays PTP foreign master records
- **show ptp parent**—Displays PTP parent properties
- **show ptp port**—Displays PTP port properties
- **show ptp time-property**—Displays PTP clock time properties



- `show interface virtual-cem 0/24`—Displays the status of the CEM interface
- `show cem circuit`—Displays information about the CEM circuit
- `show platform hardware`—Displays the status of hardware devices on the Cisco MWR 2941-DC.

## Configuring Pseudowire

This section describes how to configure pseudowire on the Cisco MWR 2941-DC. For an overview of pseudowire, see “[Cisco Pseudowire Emulation Edge-to-Edge](#)” section on page 1-2.

The Cisco MWR 2941-DC supports pseudowire connections using SAToP, CESoPSN, and ATM over MPLS. The following sections describe how to configure pseudowire connections on the Cisco MWR 2941-DC.

- [Using Pseudowire Classes](#)
- [Using CEM Classes](#)
- [Configuring Structure-Agnostic TDM over Packet \(SAToP\)](#)
- [Configuring Circuit Emulation Service over Packet-Switched Network \(CESoPSN\)](#)
- [Configuring Transportation of Service Using ATM over MPLS](#)

For full descriptions of each command, see [Appendix A, “Cisco MWR 2941-DC Router Command Reference.”](#) For pseudowire configuration examples, see [Appendix B, “Configuration Examples.”](#)

## Using Pseudowire Classes

A pseudowire class allows you to create a single configuration template for multiple pseudowire connections. You can apply pseudowire classes to SAToP, CESoPSN, and ATM over MPLS pseudowires. Follow these steps to configure a pseudowire class:

- 
- Step 1** Enter the following commands to create the pseudowire class.
- a. Enter configuration mode.  

```
Router# configure terminal
```
  - b. Use the **pseudowire-class** command to create a new pseudowire class.  

```
Router(config)# pseudowire-class newclass
```
  - c. Use the **encapsulation** command to set an encapsulation type. This example uses MPLS encapsulation for an ATM over MPLS pseudowire.  

```
Router(config-pw-class)# encapsulation mpls
```
  - d. Use the **mpls experimental** command to specify the 3-bit EXP field in the MPLS label used for pseudowire packets.  

```
Router(config-pw-class)# mpls experimental 5
```



### Note

For more information about the `mpls experimental` command, see [Appendix A, “Cisco MWR 2941-DC Router Command Reference.”](#)

---

**Step 2** Follow these steps to create a reference to the pseudowire class in the ATM IMA interface.

- a. Configure the pseudowire interface that you want to use the new pseudowire class. This example shows an ATM IMA interface.

```
Router(config)# interface atm0/ima0
Router(config-if)# pvc 0/40 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal0
```

- b. Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create an ATM pseudowire. Use the **pw-class** parameter to specify the pseudowire class that the ATM pseudowire interface uses.

```
Router(cfg-if-atm-l2trans-pvc)# xconnect 1.1.1.1 40 pw-class myclass
```

**Note**

You cannot use the encapsulation **mpls** parameter with the **pw-class** parameter.

**Note**

The use of the **xconnect** command can vary depending on the type of pseudowire you are configuring.

## Using CEM Classes

A CEM class allows you to create a single configuration template for multiple CEM pseudowires. Follow these steps to configure a CEM class:

**Note**

You cannot apply a CEM class to other pseudowire types such as ATM over MPLS.

**Step 1** Follow these steps to create the CEM class.

- a. Enter configuration mode.

```
Router# configure terminal
```

- b. Use the class cem command to create a new CEM class

```
Router(config)# class cem mycemclass
```

- c. Enter the configuration commands common to the CEM class. This example specifies a sample rate, payload size, dejitter buffer, and idle pattern.

```
Router(config-cem-class)# payload-size 512
Router(config-cem-class)# dejitter-buffer 10
Router(config-cem-class)# idle-pattern 0x55
```

- d. Type **exit** to exit the CEM class interface.

```
Router(config-cem-class)# exit
```

**Step 2** Follow these steps to create a reference to the CEM class in the CEM interface.

- a. Enter the following commands to configure the CEM interface that you want to use the new CEM class.

```
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# cem class mycemclass
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
```

**Note**

The use of the `xconnect` command can vary depending on the type of pseudowire you are configuring.

- b. Use the **exit** command to exit the CEM interface.

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

## Configuring Structure-Agnostic TDM over Packet (SAToP)

Follow these steps to configure SAToP on the Cisco MWR 2941-DC.

- 
- Step 1** Use the **controller** command to configure the T1 or E1 interface.

```
Router(config)# controller [T1|E1] 0/4
Router(config-controller)#
```

- Step 2** Use the **cem-group** command to assign channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the **unframed** parameter to assign all the T1 timeslots to the CEM channel.

```
Router(config-if)# cem-group 4 unframed
```

- Step 3** Enter the following commands to define a CEM group.

```
Router(config)# interface CEM0/4
Router(config-if)# no ip address
Router(config-if)# cem 4
```

- Step 4** Use the **xconnect** command to bind an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 304 to the remote peer 30.30.2.304.

```
Router(config-if)# xconnect 30.30.30.2 304 encapsulation mpls
```

## Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN)

Follow these steps to configure CESoPSN on the Cisco MWR 2941-DC.

- 
- Step 1** Use the **controller** command to access the E1 or T1 controller.

```
Router(config)# controller [e1|t1] 0/0
Router(config-controller)#
```

- Step 2** Use the **cem-group** command to assign channels on the T1 or E1 circuit to the circuit emulation (CEM) channel. This example uses the **timeslots** parameter to assign specific timeslots to the CEM channel.

```
Router(config-if)# cem-group 5 timeslots 1-24
```

- Step 3** Use the following commands to define a CEM channel:

```
Router(config)# interface CEM0/5
Router(config-if-cem)# cem 5
```

- Step 4** Use the **xconnect** command to bind an attachment circuit to the CEM interface to create a pseudowire. This example creates a pseudowire by binding the CEM circuit 305 to the remote peer 30.30.30.2.

```
Router(config-if-cem)# xconnect 30.30.30.2 305 encapsulation mpls
```

**Step 5** Use the **exit** command to exit the CEM interface.

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

## Configuring Transportation of Service Using ATM over MPLS

ATM over MPLS pseudowires allow you to encapsulate and transport ATM traffic across an MPLS network. This service allows you to deliver ATM services over an existing MPLS network.

The following sections describe how to configure transportation of service using ATM over MPLS:

- [Configuring the Controller](#)
- [Configuring an IMA Interface](#)
- [Configuring the ATM over MPLS Pseudowire Interface](#)
- [Optional Configurations](#)



### Note

For sample configurations for ATM over MPLS, see [“ATM over MPLS Configuration” section on page B-25](#).

## Configuring the Controller

Follow these steps to configure the controller.

**Step 1** Enter the **card type** command to configure IMA on an E1 or T1 interface.

```
Router(config)# card type e1 0 0
```

**Step 2** Specify the controller interface on which you want to enable IMA.

```
Router(config)# controller E1 0/4
Router(config-controller)#
```

**Step 3** Set the clock source to internal.

```
Router(config-controller)# clock source internal
```

**Step 4** If you want to configure an ATM IMA backhaul, use the **ima-group** command to assign the interface to an IMA group. For a T1 connection, use the **no-scrambling-payload** to disable ATM-IMA cell payload scrambling; for an E1 connection, use the **scrambling-payload** parameter to enable ATM-IMA cell payload scrambling.

The follow command assigns the interface to IMA group 0 and enables payload scrambling.

```
Router(config-controller)# ima-group 0 scrambling-payload
```



### Note

For more information about configuring IMA groups, see [Configuring ATM IMA](#). For more information about how to configure the backhaul connection, see [Configuring MLPPP Backhaul](#).

## Configuring an IMA Interface

If you want to use ATM IMA backhaul, follow these steps to configure the IMA interface.

**Step 1** Specify the slot location and port of IMA interface group.

```
Router(config-controller)# interface ATMslot/IMAgroup-number
```

- *slot*—Specifies the slot location of the ATM IMA port adapter.
- *group-number*—Specifies the group number of the IMA group.

For example, the following command specifies the slot number as 0 and the group number as 0:

```
Router(config-controller)# interface atm0/ima0
Router(config-if)#
```



**Note** To explicitly configure the IMA group ID for the IMA interface, you may use the optional **ima group-id** command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID.

**Step 2** Disable the IP address configuration for the physical layer interface.

```
Router(config-if)# no ip address
```

**Step 3** Specify the ATM bandwidth as dynamic.

```
Router(config-if)# atm bandwidth dynamic
```

**Step 4** Disable the Interim Local Management Interface (ILMI) keepalive parameters.

```
Router(config-if)# no atm ilmi-keepalive
```

For more information about configuring IMA groups, see [Configuring ATM IMA](#).

## Configuring the ATM over MPLS Pseudowire Interface

You can configure ATM over MPLS in several modes according to the needs of your network. Use the appropriate section according to the needs of your network.

- [Configuring N-to-1 VCC Cell Transport Pseudowire](#)—Maps multiple VCCs to a single pseudowire
- [Configuring N-to-1 VPC Cell Transport](#)—Maps multiple VPCs to a single pseudowire
- [Configuring ATM AAL5 SDU VCC Transport](#)—Maps a single ATM PVC to another ATM PVC
- [Configuring 1-to-1 VCC Cell Mode](#)—Maps a single VCC to a single pseudowire
- [Configuring a Port Mode Pseudowire](#)—Maps one physical port to a single pseudowire connection

### Configuring N-to-1 VCC Cell Transport Pseudowire

An N-to-1 VCC cell transport pseudowire maps one or more ATM virtual channel connections (VCCs) to a single pseudowire. Follow these steps to configure an N-to-1 pseudowire.

You can use the following methods to configure an N-to-1 VCC Cell Transport pseudowire.

- [Mapping a Single PVC to a Pseudowire](#)
- [Mapping multiple PVCs to a Pseudowire](#)

### Mapping a Single PVC to a Pseudowire

To map a single PVC to an ATM over MPLS pseudowire, apply the **xconnect** command at the PVC level. This configuration type only uses AAL0 encapsulation. Follow these steps to map a single PVC to an ATM over MPLS pseudowire.

- a. Configure the ATM IMA interface.

```
Router(config)# interface atm0/ima0
```

- b. Use the **pvc** command to define a PVC.

```
Router(config-if)# pvc 0/40
Router(cfg-if-atm-l2trans-pvc)#
```

- c. Use the **encapsulation** command to define the encapsulation type for the PVC.

```
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal0
```

- d. Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding PVC 40 to the remote peer 1.1.1.1.

```
Router(config-if)# xconnect 1.1.1.1 40 encapsulation mpls
Router(cfg-if-atm-l2trans-pvc-xconn)#
```

- e. Use the **end** command to exit configuration mode.

```
Router(cfg-if-atm-l2trans-pvp-xconn)# end
Router#
```

### Mapping multiple PVCs to a Pseudowire

To map a multiple PVCs to a single ATM over MPLS pseudowire, apply the **xconnect** command at the subinterface level. This configuration allows you to group pseudowires logically, such as by the BTS to which the pseudowire is connected. Follow these steps to map a multiple PVCs to an ATM over MPLS pseudowire.



#### Note

If you configure multiple PVCs on an N-to-1 subinterface pseudowire, you must use AAL0 encapsulation for all of the PVCs..



#### Note

When you configure a N-to-1 pseudowire, you can also use the **ignore-vpi-vci** parameter. This parameter sets the Cisco MWR 2941-DC to ignore the VPI/VCI value in the PW packet and rewrite the egress ATM cell header with VPI/VCI value of the locally configured (attachment side) PVC. For more information about the xconnect command and the ignore-vpi-vci parameter, see [Appendix A, “Cisco MWR 2941-DC Router Command Reference.”](#)

- a. Configure the ATM IMA interface.

```
Router(config)# interface atm0/ima0
```

- a. Enter the following command to create an ATM IMA multipoint subinterface.

```
Router(config-if)# interface atm 0/ima0.1 multipoint
Router(config-subif)#
```

- b. Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 100 to the remote peer 1.1.1.1.

```
Router(config-subif)# xconnect 1.1.1.1 100 encapsulation mpls
Router(config-subif-xconn)#
```

- c. Use the **exit** command to exit the xconnect subinterface.

```
Router(config-subif-xconn)# exit
Router(config-subif)#
```

- d. Use the **pvc** command to map a PVC to a pseudowire.

```
Router(config-if)# pvc 0/40 l2transport
Router(cfg-if-atm-l2trans-pvc)#
```

- e. Use the **encapsulation** command to define the encapsulation type for the PVC.

```
Router(config-if-atm-vc)# encapsulation aal0
```

- f. Define additional PVCs as appropriate. We recommend that you include a description for each PVC

```
Router(config-if)# pvc 0/41 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal0
Router(cfg-if-atm-l2trans-pvc)# description voice channel
Router(cfg-if-atm-l2trans-pvc)# exit
Router(config-subif)#pvc 0/42 l2transport
Router(cfg-if-atm-l2trans-pvc)#enc aal0
Router(cfg-if-atm-l2trans-pvc)# description data channel
```

### Configuring N-to-1 VPC Cell Transport

An N-to-1 VPC cell transport pseudowire maps one or more ATM virtual path connections (VPCs) to a single pseudowire. While the configuration is similar to one-to-one VPC cell mode, this transport method uses the N-to-1 VPC Pseudowire protocol and format defined in RFCs 4717 and 4446. Follow these steps to configure an N-to-1 VPC pseudowire.

---

#### Step 1 Configure the ATM IMA interface.

```
Router(config)# interface atm0/ima0
Router(config-if)#
```

#### Step 2 Use the **atm pvp** command to map a PVP to a pseudowire

```
Router(config-if)# atm pvp 10 l2transport
Router(cfg-if-atm-l2trans-pvp)#
```

#### Step 3 Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 305 to the remote peer 30.30.30.2.

```
Router(cfg-if-atm-l2trans-pvp)# xconnect 30.30.30.2 305 encapsulation mpls
Router(cfg-if-atm-l2trans-pvp-xconn)#
```

#### Step 4 Use the **end** command to exit configuration mode.

```
Router(cfg-if-atm-l2trans-pvp-xconn)# end
Router#
```

---

**Configuring ATM AAL5 SDU VCC Transport**

An ATM AAL5 SDU VCC transport pseudowire maps a single ATM PVC to another ATM PVC. Follow these steps to configure an ATM AAL5 SDU VCC transport pseudowire.

- Step 1** Configure the ATM IMA interface.

```
Router(config)# interface atm 0/ima0
Router(config-if)#
```

- Step 2** Use the **pvc** command to configure a PVC and specify a VCI/VPI.

```
Router(config-if)# pvc 0/12 12transport
Router(cfg-if-atm-12trans-pvc)#
```

- Step 3** Use the **encapsulation** command to set the PVC encapsulation type to AAL5.

```
Router(cfg-if-atm-12trans-pvc)# encapsulation aal5
```



**Note** You must use AAL5 encapsulation for this transport type.

- Step 4** Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 125 to the remote peer 25.25.25.25.

```
Router(cfg-if-atm-12trans-pvc)# xconnect 25.25.25.25 125 encapsulation mpls
```

**Configuring 1-to-1 VCC Cell Mode**

A VCC 1-to-1 pseudowire allows you to map a single ATM VCC to a single pseudowire. You must use AAL0 encapsulation for this transport type. Follow these steps to configure a 1-to-1 pseudowire.

- Step 1** Configure the ATM IMA interface.

```
Router(config)# interface atm 0/ima0
Router(config-if)#
```

- Step 2** Use the **pvc** command to configure a PVC and specify a VCI/VPI.

```
Router(config-if)# pvc 0/12 12transport
Router(cfg-if-atm-12trans-pvc)#
```

- Step 3** Use the **encapsulation** command to set the PVC encapsulation type to AAL0.

```
Router(cfg-if-atm-12trans-pvc)# encapsulation aal0
```



**Note** You must use AAL0 encapsulation for this transport type.

- Step 4** Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 125 to the remote peer 25.25.25.25.

```
Router(cfg-if-atm-12trans-pvc)# xconnect 25.25.25.25 125 encapsulation mpls one-to-one
```



### Configuring a Port Mode Pseudowire

A port mode pseudowire allows you to map an entire ATM interface to a single pseudowire connection. Follow these steps to configure a port mode pseudowire:

---

**Step 1** Configure the ATM interface.

```
Router(config)# interface atm 0/ima0
```

**Step 2** Use the **xconnect** command to bind an attachment circuit to the ATM IMA interface to create a pseudowire. This example creates a pseudowire by binding the ATM circuit 200 to the remote peer 25.25.25.25.

```
Router(cfg-if)# xconnect 25.25.25.25 2000 encapsulation mpls
```

---

### Optional Configurations

You can apply the following optional configurations to a pseudowire link.

- [Configuring Cell Packing](#)
- [Configuring PVC Mapping](#)

#### Configuring Cell Packing

Cell packing allows you to improve the efficiency of ATM-to-MPLS conversion by packing multiple ATM cells into a single MPLS packet. Follow these steps to configure cell packing.

---

**Step 1** Use the **atm mcpt-timers** command to define the three Maximum Cell Packing Timeout (MCPT) timers under an ATM interface. The three independent MCPT timers specify a wait time before forwarding a packet.

```
Router(config)# int atm1/0
Router(config-if)# atm mcpt-timers 1000 2000 3000
```

**Step 2** Use the **cell-packing** command to specify the maximum number of cells in PW cell pack and the cell packing timer that the Cisco MWR 2941-DC uses. This example specifies 20 cells per pack and the third MCPT timer.

```
Router(config)# pvc 0/11 l2transport
Router(cfg-if-atm-l2trans-pvc)# encapsulation aal0
Router(cfg-if-atm-l2trans-pvc)# cell-packing 20 mcpt-timer 3
```

#### Configuring PVC Mapping

PVC mapping allows you to map PVCs from multiple cell site routers to equivalent PVCs on a single aggregation node.

**Note**

PVC mapping only applies to N-to-1 cell mode and port mode. You can achieve a similar effect for AAL 5SDU mode and VCC one-to-one mode by configuring a pseudowire between two PVCs with different VPI/VCI values on two PEs.

The following example shows how to use the **pw-pvc** command to map a the local PVCs 0/11 and 0/12 to the remote PVCs 0/11 and 0/12.

```
(config)# int atm1/0
(config-if)# xconnect 25.25.25.25 2000 encapsulation mpls
```

```
(config-if)# pvc 0/11 l2transport
(cfg-if-atm-l2trans-pvc)# encapsulation aal0
(cfg-if-atm-l2trans-pvc)# pw-pvc 1/11
(config-if)# pvc 0/12 l2transport
(cfg-if-atm-l2trans-pvc)# encapsulation aal0
(cfg-if-atm-l2trans-pvc)# pw-pvc 1/12
```

## Configuring MLPPP Backhaul

To configure an MLPPP backhaul, complete the following tasks:

- [Configuring the Card Type, page 4-22](#)
- [Configuring E1 Controllers, page 4-23](#)
- [Configuring T1 Controllers, page 4-25](#)
- [Configuring Multilink Backhaul Interface, page 4-26](#)
- [Configuring the PPP Backhaul Interfaces, page 4-29](#)

## Configuring the Card Type

Perform a basic card type configuration by enabling the router, enabling an interface, and specifying the card type as described below. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

For information about interface numbering, see [Understanding the Cisco MWR 2941-DC Router Interface Numbering, page 3-1](#).



### Note

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the Router# prompt.

To select and configure a card type, follow these steps:

---

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to Router, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#
```

When the prompt changes to Router(config), you have entered global configuration mode.

**Note**

To view a list of the configuration commands available to you, enter **?** at the prompt or press the **Help** key while in configuration mode.

**Step 4** Set the card type.

```
Router(config-if)# card type {e1 | t1} slot subslot
```

- *slot*—Slot number of the interface.
- *subslot*—Specifies the VWIC slot number.

For example, the following command shows how to configure a T1/E HWIC in the first HWIC slot as an E1 card:

```
Router(config)# card type e1 0 1
```

When the command is used for the first time, the configuration takes effect immediately. A subsequent change in the card type does not take effect unless you enter the **reload** command or reboot the router.

**Note**

When you are using the **card type** command to change the configuration of an installed card, you must first enter the **no card type {e1 | t1} slot subslot** command. Then enter the **card type {e1 | t1} slot subslot** command for the new configuration information.

## Configuring E1 Controllers

Perform a basic E1 controller configuration by specifying the E1 controller, entering the clock source, specifying the channel-group, configuring the serial interface, configuring PPP encapsulation, and enabling keepalive packets. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure the E1 controllers, follow these steps while in global configuration mode:

**Step 1** Specify the controller that you want to configure. Controller E1 0/0 maps to the T1/E1 HWIC card in HWIC slot 0.

```
Router(config)# controller e1 slot/port
```

For example, the following command shows how to specify the E1 controller as the first port of the T1/E1 HWIC card in slot 0:

```
Router(config)# controller e1 0/0  
Router(config-controller)#
```

The prompt changes to `Router(config-controller)`, when you enter controller configuration mode.

**Step 2** Specify the framing type.

```
Router(config-controller)# framing {crc4 | no-crc4}
```

**Step 3** Specify the line code format.

```
Router(config-controller)# linecode {ami | hdb3}
```

**Step 4** Enter the clocking source.

```
Router(config-controller)# clock source {line | internal} [bits]
```

- *line*—Specifies the E1 line from which the clocking is taken.
- *internal*—Specifies internal clocking.
- *bits*—Enabled Building Integrated Timing Supply (BITS) clocking.

For example, the following command shows how to configure the clock source for the E1 controller:

```
Router(config-controller)# clock source line
```



**Note** When you are using the **clock source** command to change the configuration of an installed card, you must enter the **no clock source** command first. Then enter the **clock source** command for the new configuration information.

**Step 5** Specify the channel-group and time slots to be mapped. After you configure a channel-group, the serial interface is automatically created.

```
Router(config-controller)# channel-group channel-no timeslots timeslot-list speed {64}
```

- *channel-no*—ID number to identify the channel group. The valid range is 0 to 30.
- *timeslot-list*—Timeslots (DS0s) to include in this channel group. The valid timeslots are 1 to 31.
- **speed {64}**—The speed of the DS0: 64 kbps.

For example, the following command configures the channel-group and time slots for the E1 controller:

```
Router(config-controller)# channel-group 0 timeslots 1-31 speed 64
```



**Note** When you are using the **channel-group channel-no timeslots timeslot-list {64}** command to change the configuration of an installed card, you must enter the **no channel-group channel-no timeslots timeslot-list speed {64}** command first. Then enter the **channel-group channel-no timeslots timeslot-list {64}** command for the new configuration information.

**Step 6** Exit controller configuration mode.

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

**Step 7** Configure the serial interface. Specify the E1 slot, port number, and channel-group.

```
Router(config)# interface serial slot/port:channel
```

When the prompt changes to `Router(config-if)`, you have entered interface configuration mode.



**Note** To see a list of the configuration commands available to you, enter `?` at the prompt or press the **Help** key while in the configuration mode.

**Step 8** To configure PPP encapsulation, enter the following command:

```
Router(config-if)# encapsulation ppp
```

**Step 9** Enable keepalive packets on the interface and specify the number of times keepalive packets are sent without a response before bringing down the interface:

```
Router(config-if)# keepalive [period [retries]]
```

**Step 10** Exit interface configuration mode.

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

## Configuring T1 Controllers

Use the following instructions to perform a basic T1 controller configuration: specifying the T1 controller, specifying the framing type, specifying the line code form, specifying the channel-group and time slots to be mapped, configuring the cable length, configuring the serial interface, configuring PPP encapsulation, and enabling keepalive packets. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.



### Note

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure the T1 interfaces, follow these steps while in the global configuration mode:

**Step 1** Specify the controller that you want to configure. Controller T1 0/0 maps to the T1/E1 HWIC card in HWIC slot 0.

```
Router(config)# controller t1 slot/port
```

**Step 2** Specify the framing type.

```
Router(config-controller)# framing esf
```

**Step 3** Specify the line code format.

```
Router(config-controller)# linecode b8zs
```

**Step 4** Specify the channel-group and time slots to be mapped. After you configure a channel-group, the serial interface is automatically created.



### Note

The default speed of the channel-group is 56.

```
Router(config-controller)# channel-group 0 timeslots 1-24 speed 56
```

**Step 5** Configure the cable length.

```
Router(config-controller)# cablelength {long [-15db | -22.5db | -7.5db | 0db] short [110ft | 220ft | 330ft | 440ft | 550ft | 600ft]}
```

**Step 6** Exit controller configuration mode.

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

**Step 7** Configure the serial interface. Specify the T1 slot (always 0), port number, and channel-group.

```
Router(config)# interface serial slot/port:channel
```

**Step 8** Enter the following command to configure PPP encapsulation.

```
Router(config-if)# encapsulation ppp
```

- Step 9** Enable keepalive packets on the interface and specify the number of times that keepalive packets will be sent without a response the interface is brought down:

```
Router(config-if)# keepalive [period [retries]]
```

- Step 10** Exit to global configuration mode.

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

## Configuring Multilink Backhaul Interface

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



### Note

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

The Cisco MWR 2941-DC router can support up to 10 E1 or T1 interfaces through the multilink interface.

Complete the following configuration tasks for a multilink backhaul interface.

- [Creating a Multilink Bundle](#), this page
- [Configuring PFC](#), page 4-27
- [Configuring ACFC](#), page 4-28
- [Enable Multilink and Identify the Multilink Interface](#), page 4-28
- [Enable Real-Time Transport Protocol \(RTP\) Header-Compression](#), page 4-29

## Creating a Multilink Bundle

To create a multilink bundle, follow these steps, while in the global configuration mode:

- Step 1** Create a multilink bundle and enter the interface configuration mode:

```
Router(config)# interface multilink group-number
```

- *group-number*—Number of the multilink bundle.

For example, the following command creates a multilink bundle 5:

```
Router(config)# interface multilink5  
Router(config-if)#
```

To remove a multilink bundle, use the **no** form of this command.



### Note

To see a list of the configuration commands available to you, enter **?** at the prompt or press the **Help** key while in the configuration mode.

- Step 2** Assign an IP address to the multilink interface.

```
Router(config-if)# ip address address [subnet mask]
```

- *address*—The IP address.
- *subnet mask*—Network mask of IP address.

For example, the following command creates an IP address and subnet mask:

```
Router(config-if)# ip address 10.10.10.2 255.255.255.0
```

## Handling PFC and ACFC

Protocol-Field-Compression (PFC) and Address-and-Control-Field-Compression (ACFC) are PPP compression methods defined in RFCs 1661 and 1662. PFC allows for compression of the PPP Protocol field; ACFC allows for compression of the PPP Data Link Layer Address and Control fields.

Use the following instructions to perform PFC and ACFC handling during PPP negotiation to be configured. By default, PFC/ACFC handling is not enabled.



### Note

The recommended PFC and ACFC handling in the Cisco MWR 2941-DC router is: **acfc local request, acfc remote apply, pfc local request, and pfc remote apply.**

## Configuring PFC

To configure PFC handling during PPP negotiation, follow these steps, while in the interface configuration mode:

- Step 1** To configure how the router handles PFC in its outbound configuration requests, enter the following command:

```
Router(config-if)# ppp pfc local {request | forbid}
```

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.

For example, the following command shows how to create a method for the router to manage PFC:

```
Router(config-if)# ppp pfc local request
```

- Step 2** To configure a method for the router to use to manage the PFC option in configuration requests received from a remote peer, enter the following command:

```
Router(config-if)# ppp pfc remote {apply | reject | ignore}
```

Where:

- **apply**—PFC options are accepted and ACFC may be performed on frames sent to the remote peer.
- **reject**—PFC options are explicitly ignored.
- **ignore**—PFC options are accepted, but ACFC is not performed on frames sent to the remote peer.

For example, issuing the following command allows PFC options to be accepted:

```
Router(config)# ppp pfc remote apply
```

## Configuring ACFC

To configure ACFC handling during PPP negotiation, follow these steps, while in interface configuration mode:

- Step 1** To configure how the router handles ACFC in its outbound configuration requests, enter the following command:

```
Router(config-if)# ppp acfc local {request | forbid}
```

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.

For example, the following command creates how the router handles ACFC:

```
Router(config-if)# ppp acfc local request
```

- Step 2** To configure how the router handles the ACFC option in configuration requests received from a remote peer, enter the following command:

```
Router(config-if)# ppp acfc remote {apply | reject | ignore}
```

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.

For example, the following command allows ACFC options to be accepted:

```
Router(config-if)# ppp acfc remote apply
```

## Enable Multilink and Identify the Multilink Interface

To enable multilink and identify the multilink interface, follow these steps, while in interface configuration mode:

- Step 1** Enable multilink PPP operation.

```
Router(config-if)# ppp multilink
```

- Step 2** Specify an identification number for the multilink interface.

```
Router(config-if)# ppp multilink group group-number
```

- **group-number**—Multilink group number.

For example, the following command restricts (identifies) the multilink interface, 5, that can be negotiated:

```
Router(config-if)# ppp multilink group 5
```



- Step 3** Enable keepalive packets on the interface and specify the number of times the keepalive packets are sent without a response before bringing down the interface.

```
Router(config-if)# keepalive [period [retries]]
```

- **period**—(Optional) Integer value in seconds greater than 0. The default is 10.
- **retries**—(Optional) Specifies the number of times that the device will continue to send keepalive packets without response before bringing the interface down. Integer value greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value was specified previously, the default of 5 is used.

For example, the following command shows how to restrict (identify) the multilink interface, 5, that can be negotiated:

```
Router(config-if)# keepalive 1 5
```

## Enable Real-Time Transport Protocol (RTP) Header-Compression

To enable RTP Header Compression, follow these steps while in the interface configuration mode:

- Step 1** Enable RTP header-compression.

```
Router(config-if)# ip rtp header-compression [passive | iphc-format | ietf-format]  
[periodic-refresh]
```

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

For example, the following command enables RTP header-compression in the Internet Engineering Task Force (IETF) format by suppressing the IP ID in the RTP/UDP header compression:

```
Router(config-if)# ip rtp header-compression ietf-format ignore-id
```

## Configuring the PPP Backhaul Interfaces

Use the following instructions to perform a basic backhaul interface configuration: enabling an interface, configuring PPP encapsulation, enabling multilink PPP operation, and specifying an ID number for the multilink interface. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.



### Note

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To continue the configuration of the backhaul links for the E1 controllers, follow these steps while in the global configuration mode:

**Step 1** Configure the serial interface. Specify the E1 slot, port number, and channel-group.

```
Router(config)# interface serial slot/port:channel-group
```

Where:

- *slot*—Slot number of the interface.
- *port*—Port number of the interface.
- **channel-group**—ID number to identify the channel group.

For example, the following command identifies the serial interface located in slot 0, port 0, channel-group 0:

```
Router(config)# interface serial0/0:0  
Router(config-if)#
```



**Note** To view a list of available configuration commands, enter **?** at the prompt or press the **Help** key while in configuration mode.

**Step 2** Do not assign an IP address and subnet mask to the interface.

```
Router(config-if)# no ip address ip_address subnet_mask
```

**Step 3** To configure PPP encapsulation, enter the following command:

```
Router(config-if)# encapsulation ppp
```

**Step 4** Enable multilink PPP operation.

```
Router(config-if)# ppp multilink
```

**Step 5** Specify an identification number for the multilink interface.

```
Router(config-if)# ppp multilink group group-number
```

- *group-number*—Multilink group number.

For example, the following command shows how to restrict (identify) the multilink interface, 5, that can be negotiated:

```
Router(config-if)# ppp multilink group 5
```

**Step 6** Enable keepalive packets on the interface and specify the number of times the keepalive packets is sent without a response before bringing down the interface.

```
Router(config-if)# keepalive [period]
```

- *period*—(Optional) Integer value in seconds greater than 0. The default is 10.

For example, the following command indicates the number of times the keepalive packets will be sent as 1:

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

## Configuring GSM-Abis Links



### Note

The following is an example of configuring an E1 on a Cisco T1/E1 HWIC card in a Cisco MWR 2941-DC router.

Use the following instructions to perform a basic GSM-Abis configuration on a Cisco T1/E1 HWIC card located in the Cisco MWR 2941-DC router, by entering the following Cisco IOS commands at the router prompt (see the [“Understanding the Cisco MWR 2941-DC Router Interface Numbering”](#) section on [page 3-1](#) for information about slot and port numbering on the Cisco MWR 2941-DC router). You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.



### Note

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure the GSM-Abis attributes, follow these steps while in global configuration mode:

**Step 1** Set the card type for the Cisco T1/E1 HWIC card.

```
Router(config)# card type {e1 | t1} slot subslot
```

- **e1**—Card type E1.
- **t1**—Card type T1.
- *slot*—Slot number of the interface.
- *subslot*—Specifies the Cisco T1/E1 HWIC interface card (HWIC slot) port number.

The following command configures the Cisco T1/E1 HWIC card located in the HWIC slot 0 as an E1:

```
Router(config)# card type e1 0 1
```

When the command is used for the first time, the configuration takes effect immediately. A subsequent change in the card type does not take effect unless you enter the **reload** command or reboot the router.

**Step 2** Specify the controller that you want to configure by entering the controller configuration mode. Controller E1 0/0 maps to the Cisco T1/E1 HWIC card located in HWIC slot 0.



### Note

For more information about interface numbering, see [“Understanding the Cisco MWR 2941-DC Router Interface Numbering”](#) section on [page 3-1](#).

```
Router(config)# controller e1 slot/port
```

- *slot*—The HWIC slot where the T1/E1-RAN card is installed.
- *port*—Number of the serial port the T1/E1-RAN card is using.

For example, the following command specifies the E1 controller as the Cisco T1/E1 HWIC card located in HWIC slot 0:

```
Router(config)# controller e1 0/2  
Router(config-controller)#
```

**Step 3** Enter the clocking source. For more information on clocking, see [Configuring Network Clocking Support](#), [page 4-6](#).

```
Router(config-controller)# clock source {line | internal}
```

- **line**—Specifies the E1 line from which the clocking is taken.
- **internal**—Specifies internal clocking.

For example, the following command configures the clock source for the E1 controller:

```
Router(config-controller)# clock source internal
```



**Note** When you are using the **clock source** command to change the configuration of an installed card, you must enter the **no clock source** command first. Then enter the **clock source** command for the new configuration information.

- Step 4** Specify the channel-group and time slots to be mapped. After you configure a channel-group, the serial interface is automatically created.



**Note** You can only create one channel group per E1 or T1 interface.

```
Router(config-controller)# channel-group channel-no timeslots timeslot-list speed {64}
```

- *channel-no*—ID number to identify the channel group. The valid range is 0 to 30.
- *timeslot-list*—Timeslots (DS0s) to include in this channel group. The valid timeslots are 1 to 31 and must be contiguous.
- **speed {64}**—The speed of the DS0: 64 kbps.

For example, the following command configures the channel-group and time slots for the E1 controller:

```
Router(config-controller)# channel-group 0 timeslots 1-31 speed 64
```



**Note** When you are using the **channel-group** *channel-no* **timeslots** *timeslot-list* **{64}** command to change the configuration of an installed card, you must enter the **no channel-group** *channel-no* **timeslots** *timeslot-list* **speed {64}** command first. Then enter the **channel-group** *channel-no* **timeslots** *timeslot-list* **{64}** command for the new configuration information.

- Step 5** Exit back to global configuration mode.

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

- Step 6** To configure the GSM-Abis interface, first specify the serial interface that you want to configure by entering the interface configuration mode.

```
Router(config)# interface serial slot/port:channel-group
```

- *slot*—Number of the slot being configured.
- *port*—Number of the port being configured.
- *channel-group*—Specifies the E1 channel group number defined with the channel-group controller configuration command.

For example, the following command enables the serial interface on HWIC-2, port 0:

```
Router(config)# interface serial 0/2:0
Router(config-if)#
```

**Note**

To view a list of available configuration commands, enter **?** at the prompt or press the **Help** key while in the configuration mode.

- Step 7** Enter the following command to configure GSM-Abis interface encapsulation in interface configuration mode.

```
Router(config-if)# encapsulation gsm-abis
```

- **gsm-abis**—Type of interface layer.

For example, the following command enables encapsulation on the GSM-Abis interface layer:

```
Router(config-if)# encapsulation gsm-abis
```

- Step 8** To configure the local parameters required to establish an IP/UDP backhaul connection, enter the following command including the IP address and port you want to establish the IP/UDP backhaul connection from in the interface configuration mode.

```
Router(config-if)# gsm-abis local ip-address port
```

- **ip-address**—The IP address for the entry you wish to establish.
- **port**—The port you want to use for the entry you wish to establish.

For example, the following command configures the **gsm-abis local** parameters to an IP address of 10.10.10.2 located on port 5502:

```
Router(config-if)# gsm-abis local 10.10.10.2 5502
```

- Step 9** To configure the remote parameters required to establish an IP/UDP backhaul connection, enter the following command including the IP address and port you want to establish the IP/UDP backhaul connection to in the interface configuration mode.

```
Router(config-if)# gsm-abis remote ip-address port
```

- **ip-address**—The IP address for the entry you wish to establish.
- **port**—The port you want to use for the entry you wish to establish.

For example, the following command configures the **gsm-abis remote** parameters to an IP address of 10.10.10.1 located on port 5502:

```
Router(config-if)# gsm-abis remote 10.10.10.1 5502
```

- Step 10** Exit the interface configuration mode.

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

## Configuring SNMP Support

Use the following instructions to configure SNMP support: setting up the community access, establishing a message queue for each trap host, enabling the router to send SNMP traps, enabling SNMP traps for alarms, and enabling SNMP traps for a specific environment. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure a Cisco MWR 2941-DC for SNMP, follow these steps while in the global configuration mode:

- Step 1** To set up the community access string to permit access to the SNMP, use the **snmp-server community** command. The **no** form of this command removes the specified community string.

```
Router(config)# snmp-server community string [view view-name] [ro | rw] [number]
```

- *string*—Community string that acts like a password and permits access to the SNMP protocol.
- **view view-name**—(Optional) Name of a previously defined view. The view defines the objects available to the community.
- **ro**—(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw**—(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
- *number*—(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

For example, the following command sets up the community access string as `xxxxx` with read-only access:

```
Router(config)# snmp-server community xxxxx RO
```

- Step 2** To establish the message queue length for each trap host, use the **snmp-server queue-length** command.

```
Router(config)# snmp-server queue-length length
```

- *length*—Integer that specifies the number of trap events that can be held before the queue must be emptied.

For example, the following command establishes the number of trap events to 100:

```
Router(config)# snmp-server queue-length 100
```

- Step 3** To enable the router to send SNMP traps or informs (SNMP notifications), use the **snmp-server enable traps** command. Use the **no** form of this command to disable SNMP notifications.

```
Router(config)# snmp-server enable traps [notification-type] [notification-option]
```

- **notification-type—snmp [authentication]**—Enables RFC 1157 SNMP notifications. Note that use of the **authentication** keyword produces the same effect as not using the **authentication** keyword. Both the **snmp-server enable traps snmp** and **snmp-server enable traps snmp authentication** forms of this command will globally enable (or, if using the **no** form, disable) the following SNMP traps:
  - authentication failure
  - linkup
  - linkdown
  - coldstart
  - warmstart

- **notification-option**—(Optional) **atm pvc** [*interval seconds*] [*fail-interval seconds*]—The optional interval seconds keyword/argument combination specifies the minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval to prevent trap storms. No traps are sent until the interval lapses. The default interval is 30.

The optional fail-interval seconds keyword/argument combination specifies the minimum period for storing the failed time stamp, in the range from 0 to 3600. The default fail-interval is 0.

**envmon** [**voltage** | **shutdown** | **supply** | **fan** | **temperature**]—When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**.

**isdn** [**call-information** | **isdn u-interface**]—When the **isdn** keyword is used, you can specify the **call-information** keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdnu-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem.

**repeater** [**health** | **reset**]—When the **repeater** keyword is used, you can specify the **repeater** option. If no option is specified, all repeater notifications are enabled. The option can be one or more of the following keywords:

- **health**—Enables IETF Repeater Hub MIB (RFC 1516) health notification.
- **reset**—Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

For example, the following command enables traps for SNMP link down, link up, coldstart, and warmstart:

```
Router(config)# snmp-server enable traps snmp linkdown linkup coldstart warmstart
```

**Step 4** To enable SNMP traps for all IP-RAN notifications, enter:

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



**Note**

Besides enabling SNMP traps for all IP-RAN notifications, you can also enable traps for IP-RAN GSM alarms, UMTS alarms, and general information about the backhaul utilization (see [Appendix A, “Cisco MWR 2941-DC Router Command Reference”](#) for descriptions on how to use these SNMP commands.

**Step 5** To enable SNMP traps for a specific environment, enter:

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

**Step 6** To specify the recipient of an SNMP notification operation, use the **snmp-server host** command. To remove the specified host, use the **no** form of this command.

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

- **host-addr**—Name or Internet address of the host (the targeted recipient).
- **traps**—(Optional) Send SNMP traps to this host. This is the default.
- **informs**—(Optional) Send SNMP informs to this host.
- **version**—(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword. If you use the version keyword, one of the following must be specified:
  - **1**—SNMPv1. This option is not available with informs.

- **2c**—SNMPv2C.
- **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword:
  - **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication
  - **noauth** (Default). The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified.
  - **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
- *community-string*—Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command before using the **snmp-server host** command.
- **udp-port** *port*—UDP port of the host to use. The default is 162.
- *notification-type*—(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:
  - **aaa\_server**—Enable SNMP AAA Server traps.
  - **atm**—Enable SNMP atm Server traps.
  - **ccme**—Enable SNMP ccme traps.
  - **cnpd**—Enable NBAR Protocol Discovery traps.
  - **config**—Enable SNMP config traps.
  - **config-copy**—Enable SNMP config-copy traps.
  - **cpu**—Allow cpu related traps.
  - **dial**—Enable SNMP dial control traps.
  - **dnis**—Enable SNMP DNIS traps.
  - **ds0-busyout**—Enable ds0-busyout traps.
  - **ds1**—Enable SNMP DS1 traps.
  - **ds1-loopback**—Enable ds1-loopback traps.
  - **ds3**—Enable SNMP DS3 traps.
  - **dsp**—Enable SNMP dsp traps.
  - **eigrp**—Enable SNMP EIGRP traps.
  - **entity**—Enable SNMP entity traps.
  - **envmon**—Enable SNMP environmental monitor traps.
  - **flash**—Enable SNMP FLASH notifications.
  - **frame-relay**—Enable SNMP frame-relay traps.
  - **hsrp**—Enable SNMP HSRP traps.
  - **icsudsu**—Enable SNMP ICSUDSU traps.
  - **ipmulticast**—Enable SNMP ipmulticast traps.
  - **ipran**—Enable IP-RAN Backhaul traps.
  - **ipsla**—Enable SNMP IP SLA traps.
  - **isdn**—Enable SNMP isdn traps.



- **12tun**—Enable SNMP L2 tunnel protocol traps.
- **mpls**—Enable SNMP MPLS traps.
- **msdp**—Enable SNMP MSDP traps.
- **mvpn**—Enable Multicast Virtual Private Networks traps.
- **ospf**—Enable OSPF traps.
- **pim**—Enable SNMP PIM traps.
- **pppoe**—Enable SNMP pppoe traps.
- **pw**—Enable SNMP PW traps.
- **rsvp**—Enable RSVP flow change traps.
- **snmp**—Enable SNMP traps.
- **srst**—Enable SNMP srst traps.
- **syslog**—Enable SNMP syslog traps.
- **tty**—Enable TCP connection traps.
- **voice**—Enable SNMP voice traps.
- **vrrp**—Enable SNMP vrrp traps.
- **vtp**—Enable SNMP VTP traps.
- **xgcp**—Enable XGCP protocol traps.

For example, the following command specifies a recipient of the SNMP operation with a host-address of 10.20.30.40 with a version SNMP of SNMPv2C:

```
Router(config)# snmp-server host 10.20.30.40 version 2c
```

**Step 7** Exit the global configuration mode.

```
Router(config)# exit
```

## Configuring ATM IMA

The Inverse Multiplexing for ATM (IMA) interface feature as a shorthaul is implemented in Cisco IOS Release 12.4(19)MR2. For more information on the commands used in this section, see [Appendix A, “Cisco MWR 2941-DC Router Command Reference.”](#)

Inverse multiplexing provides the capability to transmit and receive a single high-speed data stream over multiple slower-speed physical links. In inverse multiplexing over ATM (IMA), the originating stream of ATM cells is divided so that complete ATM cells are transmitted in round-robin order across the set of ATM links. IMA is supported on the Cisco T1/E1 HWIC on the Cisco MWR 2941-DC router.

**Step 1** Enter the **card type** command to configure IMA on an E1 or T1 interface.

```
Router(config)# card type e1 0 0
```

**Step 2** Specify the controller interface on which you want to enable IMA.

```
Router(config)# controller E1 0/4
Router(config-controller)#
```

**Step 3** Set the clock source to internal.

```
Router(config-controller)# clock source internal
```

**Step 4** Use the `ima-group` command to assign the interface to an IMA group, and set the scrambling-payload parameter to randomize the ATM cell payload frames. This command assigns the interface to IMA group 0.

```
Router(config-controller)# ima-group 0 scrambling-payload
```




---

**Note** This command automatically creates an ATM0/IMAx interface.

---

**Step 5** To add another member link, repeat [Step 1](#) to [Step 4](#).

**Step 6** Type `exit` to exit the controller interface.

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

**Step 7** Specify the slot location and port of IMA interface group.

```
Router(config-if)# interface ATMslot/IMA<group-number>
```

- *slot*—Specifies the slot location of the ATM IMA port adapter.
- *group-number*—Specifies the group number of the IMA group.

For example, the following command specifies the slot number as 0 and the group number as 0:

```
Router(config-if)# interface atm0/ima0
```




---

**Note** To explicitly configure the IMA group ID for the IMA interface, you may use the optional **ima group-id** command. You cannot configure the same IMA group ID on two different IMA interfaces; therefore, if you configure an IMA group ID with the system-selected default ID already configured on an IMA interface, the system toggles the IMA interface to make the user-configured IMA group ID the effective IMA group ID. At the same, the system toggles the original IMA interface to select a different IMA group ID.

---

**Step 8** Disable the IP address configuration for the physical layer interface.

```
Router(config-if)# no ip address
```

**Step 9** Specify the ATM bandwidth as dynamic.

```
Router(config-if)# atm bandwidth dynamic
```

**Step 10** Disable the Interim Local Management Interface (ILMI) keepalive parameters.

```
Router(config-if)# no atm ilmi-keepalive
```




---

**Note** The above configuration has one IMA shorthaul with two member links (atm0/0 and atm0/1).

---

## Configuring BFD

Bidirectional Forwarding Detection (BFD) provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. Cisco supports the BFD asynchronous mode, in which two routers exchange BFD control packets to activate and maintain BFD neighbor sessions. To create a BFD session, you must configure BFD on both systems (or BFD peers). Once you have enabled BFD on the interface and the router level for the appropriate routing protocols, a BFD session is created, BFD timers are negotiated, and the BFD peers begin to send BFD control packets to each other at the negotiated interval.

### Configuring BFD for OSPF

This section describes how to configure BFD on the Cisco MWR 2941-DC.

#### Configuring BFD for OSPF on a Single Interface

Follow these steps to configure BFD for OSPF on a single interface.

- 
- Step 1** Enter enable mode.
- ```
Router> enable
```
- Step 2** Enter the password.
- ```
Password: password
```
- When the prompt changes to `Router`, you have entered enable mode.
- Step 3** Enter global configuration mode.
- ```
Router# configure terminal
```
- Enter configuration commands, one per line. End with CNTL/Z.
- Step 4** Use the **interface** command to specify the interface you wish to configure.
- ```
Router(config)# interface vlan1
Router(config-if)#
```
- Step 5** Use the **bfd interval** command to specify the BFD interval.
- ```
Router(config-if)# bfd interval milliseconds min_rx milliseconds multiplier
interval-multiplier
```
- *milliseconds*—Specifies the transmit interval between BFD packets.
  - *milliseconds*—Specifies the minimum receive interval capability.
  - *interval-multiplier*—Specifies the multiplier used to calculate the holddown time.
- Step 6** Use the **ip ospf bfd** command to enable BFD for OSPF.
- ```
Router(config-if)# ip ospf bfd
```

**Note**

You can also use the `show bfd neighbors` and `show ip ospf` commands to display troubleshooting information about BFD and OSPF.

For a sample BFD configuration, see [Appendix B, “Configuration Examples.”](#)

For more information about BFD, refer to the *Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T*.

## Configuring BFD for OSPF on All Interfaces

**Step 1** Enter enable mode.

```
Router> enable
```

**Step 2** Enter the password.

```
Password: password
```

When the prompt changes to `Router`, you have entered enable mode.

**Step 3** Enter global configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

**Step 4** Use the `router ospf process-id` command to create a configuration for an OSPF process.

```
Router(config)# router ospf 100
```

**Step 5** Use the `bfd all-interfaces` command to enable BFD globally on all interfaces associated with the OSPF routing process.

```
Router(config)# bfd all-interfaces
```

**Note**

You can disable BFD on a single interface using the `ip ospf bfd disable` command on the relevant interface.

For a sample BFD configuration, see [Appendix B, “Configuration Examples.”](#)

For more information about BFD, refer to the *Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T*.

## Configuring Satellite Support in a RAN-O Network

To support the configuration of a RAN-O network when satellites are employed, you must implement a configurable jitter buffer and a tunable retransmission timer of repetitive sub-rates to overcome the network latency and satellite signal fade.

Use the following instructions to perform a GSM-Abis configuration with satellite support on the Cisco T1/E1 HWIC card with the Cisco MWR 2941-DC router. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure the GSM-Abis attributes with satellite support, follow these steps while in global configuration mode:

**Step 1** Perform Steps 1 through 10 as described in the previous procedure (see the [“Configuring GSM-Abis Links” procedure on page 4-31](#)).

**Step 2** To configure the jitter buffer, enter the following command including the value of the jitter buffer.

```
Router(config-if)# gsm-abis jitter value
```

- *ms*—The value range in milliseconds of the jitter buffer. The default is 4 ms.

For example, the following command configures the **gsm-abis jitter** buffer to 10 ms:

```
Router(config-if)# gsm-abis jitter 10
```

**Step 3** To configure the tunable retransmission timer, enter the following command including the value in milliseconds to retransmit.

```
Router(config-if)# gsm-abis retransmit value
```

- *value*—The sample delay which is a value range of the retransmission of 100 ms to 5100 ms in 20 ms intervals. For example, if the value is 5, then the amount of time in ms would be calculated as 5 times 20 ms or a total of 100 ms as the retransmit time.

For example, the following command configures the **gsm-abis retransmit** timer to a value of 5 or 100 ms:

```
Router(config-if)# gsm-abis retransmit 5
```

## Configuring Graceful Degradation

A local Cisco MWR 2941-DC router detects congestion on the backhaul by measuring its transmit jitter buffer level. If the transmit jitter buffer shrinks, it means that the backhaul packets are not arriving fast enough to fill the transmit jitter buffer indicating congestion. You should set the congestion abatement detection level at which a remote router will stop suppressing these timeslots.

Use the following instructions to configure graceful degradation on the Cisco MWR 2941-DC router by entering the following Cisco IOS commands at the router prompt.

You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

**Note**

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the Router# prompt.

To configure graceful degradation, follow these steps while in the global configuration mode:

**Step 1** Perform Steps 1 through 10 as described in the previous procedure (see the [“Configuring GSM-Abis Links” procedure on page 4-31](#)).

**Step 2** To set the congestion detection algorithm to monitor the transmit jitter buffer so as to send the congestion indicator signals to the remote when the congestion is detected, enter the following command.

```
Router(config-if)# gsm-abis congestion enable
```

**Step 3** To set the congestion abate detection level, enter the following command.

```
Router(config-if)# gsm-abis congestion abate ms
```

- *ms*—The value of the congestion abate in milliseconds.

For example, the following command configures the **gsm-abis congestion abate** detection level to a value 250 ms:

```
Router(config-if)# gsm-abis congestion abate 250
```

**Note**

The abate detection level is defined as x milliseconds of continuous congestion abatement (that is, no congestion indications).

**Step 4** To set the congestion onset detection level at which the remote router will start suppressing all timeslots that are not defined as critical in an effort to alleviate the congestion, enter the following command.

```
Router(config-if)# gsm-abis congestion onset ms
```

- *ms*—The value of the congestion onset in milliseconds.

For example, the following command configures the **gsm-abis congestion onset** detection level to a value 100 ms:

```
Router(config-if)# gsm-abis congestion onset 100
```

**Note**

The onset detection level is defined as x milliseconds of continuous congestion detected.

- Step 5** To define the critical timeslots that are exempt from suppression during congestion onset, enter the following command.

```
Router(config-if) # gsm-abis congestion critical timeslot-range
```

- *timeslot-range*—Specifies a value or range of values for time slots that are exempt from suppression during congestion onset. Use a hyphen to indicate a range.

For example, the following command configures the **gsm-abis congestion critical** timeslot range as 1-10:

```
Router(config-if) # gsm-abis congestion critical 1-10
```

**Note**

These are the timeslots that contain signalling and control information exchanged between the BSC and BTS.

## Configuring Link Noise Monitor

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 Cisco MWR 2941-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.

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.

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 **lcw** keyword, the duration must be configured after the LCV threshold. For example, **span warn lcw 55 duration 20** is a correct way to issue the command; **span warn duration 20 lcw 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.

## 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 and/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>

## Saving Configuration Changes

After you have completed configuring your Cisco MWR 2941-DC router, to prevent the loss of the router configuration, you must store the configuration changes by saving it to NVRAM so that the router boots with the configuration you entered.

---

**Step 1** Exit the global configuration mode.

```
Router(config)# exit
```

**Tip**

To return immediately to enable mode (`Router#`), press **Ctrl-Z** in any mode instead of entering **exit**, which returns you to the mode you were in previously.

- Step 2** Save the configuration changes to NVRAM so that they are not lost during resets, power cycles, or power outages.

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

## Monitoring and Managing the Cisco MWR 2941-DC Router

The following sections describe how to monitor and manage the Cisco MWR 2941-DC.

- [Using Cisco Mobile Wireless Transport Manager \(MWTM\)](#)
- [Enabling the Cisco MWR 2941-DC Router for Remote Network Management](#)
- [Show Commands for Monitoring the Cisco MWR 2941-DC Router](#)

### Using Cisco Mobile Wireless Transport Manager (MWTM)

You can use Cisco network management applications, such as Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco MWR 2941-DC. This Network Management tool provides monitoring and management capabilities to the RAN-O solution. The Cisco MWTM addresses the element-management requirements of mobile operators and provides fault, configuration, and troubleshooting capability. The Cisco MWTM provides the following key features:

- Event Monitoring
- Web-Based Reporting
- Autodiscovery and Topology
- Inventory
- OSS Integration
- Security
- Client/Server Architecture
- Multiple OS Support

The Cisco MWTM integrates with any SNMP-based monitoring system, such as Cisco Info Center products. In addition, the Cisco MWTM collects a large amount of performance data that can be exported or directly accessed from the database. This data can then be used by performance reporting applications. For more information about MWTM, see

[http://www.cisco.com/en/US/products/ps6472/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html).

### Enabling the Cisco MWR 2941-DC Router for Remote Network Management

To enable remote network management of the Cisco MWR 2941-DC, do the following:

- Step 1** At the privileged EXEC prompt, enter the following command to access the 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 (see the “[Configuring Gigabit Ethernet Interfaces](#)” section on page 4-4 for more information):

```
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 Cisco Info Center workstation with the **ip host** command in [Step 2](#).



**Note** See the “[Configuring SNMP Support](#)” section on page 4-33 for more information about configuring Steps 5 through 8 in this procedure.

- 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
```

## Show Commands for Monitoring the Cisco MWR 2941-DC Router

To monitor and maintain the Cisco MWR 2941-DC router, use the following commands:

Command	Purpose
<b>show atm cell-packing</b>	Information about Layer 2 transport ATM cell-packing.
<b>show cem circuit</b>	Summary about the CEM circuit state, including controller, interface, and AC.  Also displays specific CEM circuit state, circuit parameters, and statistics/counters.
<b>show cem platform</b>	CEM errors and information.
<b>show controllers</b>	All network modules and their interfaces. Also displays the status of the VWIC relays when a VWIC is installed.
<b>show controllers gigabitethernet <i>slot/port</i></b>	Information about initialization block, transmit ring, receive ring, and errors for the Fast Ethernet controller chip.
<b>show controllers e1</b>	Information about controller status specific to the controller hardware. Also displays statistics about the E1 link. If you specify a slot and a port number, statistics for each 15-minute period appears.
<b>show controllers t1</b>	Information about cable length, framing, firmware, and errors associated with the T1. With the Cisco MWR 2941-DC router, this command also shows the status of the relays on the VWIC.
<b>show gsm traffic</b>	Traffic rates in bits per second at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals for GSM data transmitted and received over the backhaul.
<b>show gsm-abis efficiency [history]</b>	The history of the GSM efficiency averages for compression/decompression at 1-second, 5-second, 1-minute, 5-minute, and 1-hour intervals.
<b>show gsm-abis errors</b>	Error statistics counters of the GSM for compression/decompression.
<b>show gsm-abis packets</b>	Packet statistics counters of the GSM for compression/decompression.
<b>show gsm-abis peering [details]</b>	Peering status, statistics, and history of the GSM compression/decompression.
<b>show interface <i>type slot/port</i></b>	Configuration and status of the specified interface.
<b>show interface virtual-cem <i>slot/port</i></b>	Displays the status of the CEM interface.
<b>show interface gigabitethernet <i>slot/port</i></b>	Status of the FE interface.

Command	Purpose
<b>show ip rtp header-compression</b>	RTP header compression statistics.
<b>show mpls l2transport vc</b>	Information about Any Transport over MPLS (AToM) virtual circuits (VCs) that are enabled to route Layer 2 packets on a router.
<b>show network-clocks</b>	Network clocking configuration.
<b>show platform hardware</b>	Displays the status of hardware devices on the Cisco MWR 2941-DC router.
<b>show ppp multilink</b>	MLP and multilink bundle information.
<b>show ppp multilink interface <i>number</i></b>	Multilink information for the specified interface.
<b>show protocols</b>	Protocols configured for the router and the individual interfaces.
<b>show ptp clock</b>	Displays ptp clock information.
<b>show ptp foreign-master-record</b>	Displays PTP foreign master records.
<b>show ptp parent</b>	Displays PTP parent properties.
<b>show ptp port</b>	Displays PTP port properties.
<b>show ptp time-property</b>	Displays PTP clock time properties.
<b>show xconnect all</b>	xconnect information.





# APPENDIX **A**

## Cisco MWR 2941-DC Router Command Reference

---

This appendix contains an alphabetical listing of new and revised commands specific to the Cisco MWR 2941-DC router.

- [backup delay](#)
- [backup peer](#)
- [cdp enable](#)
- [cem-group](#)
- [class cem](#)
- [clear gsm-abis](#)
- [clear ip rtp header-compression](#)
- [dejitter-buffer](#)
- [gsm-abis congestion abate](#)
- [gsm-abis congestion critical](#)
- [gsm-abis congestion enable](#)
- [gsm-abis congestion onset](#)
- [gsm-abis jitter](#)
- [gsm-abis local](#)
- [gsm-abis lost-recovery](#)
- [gsm-abis remote](#)
- [gsm-abis retransmit](#)
- [gsm-abis set dscp](#)
- [idle-pattern](#)
- [ima-group](#)
- [interface atm ima](#)
- [ip local interface](#)
- [ip rtp header-compression](#)
- [ip tcp header-compression](#)
- [ipran-mib backhaul-notify-interval](#)
- [ipran-mib location](#)

- `ipran-mib snmp-access`
- `ipran-mib threshold-acceptable`
- `ipran-mib threshold-overloaded`
- `ipran-mib threshold-warning`
- `keepalive`
- `load-interval`
- `match ip dscp`
- `mpls ip`
- `network-clock-select hold_timeout`
- `network-clock-select input-stratum4`
- `network-clock-select mode`
- `network-clock-select priority`
- `payload-size`
- `pseudowire-class`
- `ptp announce`
- `ptp clock-source`
- `ptp clock-destination`
- `ptp delay-req`
- `ptp domain`
- `ptp enable`
- `ptp master`
- `ptp mode`
- `ptp priority1`
- `ptp priority2`
- `ptp slave`
- `ptp sync interval`
- `ptp sync limit`
- `pw-pvc`
- `recovered-clock slave`
- `recovered-clock recovered`
- `set network-clocks`
- `show atm cell-packing`
- `show cem circuit`
- `show cem platform`
- `show connection`
- `show controller`
- `show gsm-abis efficiency`
- `show gsm-abis errors`



- [show gsm-abis packets](#)
- [show gsm-abis peering](#)
- [show gsm-abis traffic](#)
- [show interface switchport backup](#)
- [show ip rtp header-compression](#)
- [show mpls l2transport vc](#)
- [show network-clocks](#)
- [show platform hardware](#)
- [show ptp clock](#)
- [show ptp foreign-master-record](#)
- [show ptp parent](#)
- [show ptp port](#)
- [show ptp time-property](#)
- [show xconnect all](#)
- [snmp-server enable traps ipran](#)
- [snmp-server enable traps ipran alarm-gsm](#)
- [snmp-server enable traps ipran util](#)
- [switchport backup interface](#)
- [xconnect](#)
- [xconnect logging redundancy](#)

# backup delay

To specify how long a backup pseudowire (PW) virtual circuit (VC) should wait before resuming operation after the primary PW VC goes down, use the **backup delay** command in interface configuration mode or xconnect configuration mode. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

**backup delay** *enable-delay* [*disable-delay* | **never**]

**no backup delay** *enable-delay* [*disable-delay* | **never**]

<b>Syntax Description</b>	<i>enable-delay</i>	Number of seconds that elapse after the primary PW VC goes down before the Cisco IOS software activates the secondary PW VC. The range is 0 to 180. The default is 0.
	<i>disable-delay</i>	Number of seconds that elapse after the primary PW VC comes up before the Cisco IOS software deactivates the secondary PW VC. The range is 0 to 180. The default is 0.
	<b>never</b>	The secondary PW VC does not fall back to the primary PW VC if the primary PW VC becomes available again, unless the secondary PW VC fails.

<b>Defaults</b>	If a failover occurs, the xconnect redundancy algorithm immediately switches over or falls back to the backup or primary member in the redundancy group.
-----------------	--

<b>Command Modes</b>	Interface configuration Xconnect configuration
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Examples</b>	The following example shows a Multiprotocol Label Switching (MPLS) xconnect with one redundant peer. After a switchover to the secondary VC occurs, there is no fallback to the primary VC unless the secondary VC fails.
-----------------	---

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 0 never
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

The following example shows an MPLS xconnect with one redundant peer. The switchover does not begin unless the PW has been down for 3 seconds. After a switchover to the secondary VC occurs, there is no fallback to the primary until the primary VC has been reestablished and is up for 10 seconds.

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 3 10
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

**Related Commands**

Command	Description
<b>backup peer</b>	Configures a redundant peer for a PW VC.

# backup peer

To specify a redundant peer for a pseudowire (PW) virtual circuit (VC), use the **backup peer** command in interface configuration mode or xconnect configuration mode. To remove the redundant peer, use the **no** form of this command.

**backup peer** *peer-router-ip-addr* *vcid* [**pw-class** *pw-class-name*]

**no backup peer** *peer-router-ip-addr* *vcid*

## Syntax Description

<i>peer-router-ip-addr</i>	IP address of the remote peer.
<i>vcid</i>	The 32-bit identifier of the VC between the routers at each end of the layer control channel.
<b>pw-class</b>	(Optional) PW type. If not specified, the PW type is inherited from the parent xconnect.
<i>pw-class-name</i>	(Optional) Name of the PW you created when you established the PW class.

## Defaults

No redundant peer is established.

## Command Modes

Interface configuration  
Xconnect configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

The combination of the *peer-router-ip-addr* and *vcid* arguments must be unique on the router.

## Examples

The following example shows an MPLS xconnect with one redundant peer:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0
Router(config-if)# xconnect 10.0.0.1 100 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 200
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

The following example shows a backup peer configuration for an ATM interface:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
```

```
Router(config-pw-class)# exit
Router(config)# interface atm0/1
Router(config-if)# xconnect 10.0.0.2 1 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 100 pw-class mpls
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

**Related Commands**

Command	Description
<b>backup delay</b>	Specifies how long the backup PW VC should wait before resuming operation after the primary PW VC goes down.

# cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** command in interface configuration mode. To disable CDP on an interface, use the **no** form of this command.

**cdp enable**

**no cdp enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled at the global level and on all supported interfaces.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

CDP is enabled by default at the global level and on each supported interface in order to send or receive CDP information. However, some interfaces, such as ATM interfaces, do not support CDP.



### Note

The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the “On-Demand Routing Commands” chapter in the *Cisco IOS Command Reference, Volume 2 of 3: Routing Protocols* document.

## Examples

In the following example, CDP is disabled on the Ethernet 0 interface only:

```
Router# show cdp
Global CDP information
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Router# config terminal
Router(config)# interface ethernet 0
Router(config-if)# no cdp enable
```

## Related Commands

Command	Description
<b>cdp run</b>	Reenables CDP on a Cisco device.
<b>cdp timer</b>	Specifies how often the Cisco IOS software sends CDP updates.
<b>router odr</b>	Enables on-demand routing on a hub router.

# cem-group

To create a circuit emulation (CEM) channel from one or more time slots of a T1 or E1 line, use the **cem-group** command in controller configuration mode. To remove a CEM group and release the associated time slots, use the **no** form of this command.

**cem-group** *group-number* {**unframed** | **timeslots** *time-slot-range*}

**no cem-group** *group-number*

## Syntax Description

<i>group-number</i>	CEM identifier to be used for this group of time slots: <ul style="list-style-type: none"> <li>For T1 ports, the range is from 0 to 23.</li> <li>For E1 ports, the range is from 0 to 30.</li> </ul>
<b>unframed</b>	Specifies that a single CEM channel is being created, including all time slots, without specifying the framing structure of the line.
<b>timeslots</b>	Specifies that a list of time slots is to be used as specified by the <i>time-slot-range</i> argument.  <i>time-slot-range</i> —Specifies the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.

## Defaults

No CEM groups are defined.

## Command Modes

Controller configuration

## Command History

Release	Modification
12.4(12)MR2	This command was incorporated.

## Usage Guidelines

Use this command to create CEM channels on the T1 or E1 port.

## Examples

The following example shows how to create a CEM channel:

### SATOP

```
Router# config t
Router(config)# controller e1 0/0
Router(config-controller)# cem-group 0 unframed
Router(config-controller)# exit
Router(config)# interface cem 0/0
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
```

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

**CESoPSN**

```
Router# config t
Router(config)# controller e1 0/1
Router(config-controller)# cem-group 0 timeslots 1-31
Router(config-controller)# exit
Router(config)# interface cem 0/1
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

**Related Commands**

Command	Description
cem	Enters circuit emulation configuration mode.



# class cem

To configure CEM interface parameters in a class that is applied to CEM interfaces together, use the **class cem** command in global configuration mode. This command works in the same manner for CEM interfaces as the **pseudowire-class** command does for xconnect.

**class cem** *class-name*

## Syntax Description

*class-name* The name of a CEM interface parameters class.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(12)MR2	This command was incorporated.

## Usage Guidelines

The **class cem** command allows you to configure CEM interface parameters in a class that is applied to CEM interfaces together. A **class cem** command includes the following configuration settings:

- **de jitter-buffer** *de jitter-in-ms*
- **idle-pattern** *8-bit-idle-pattern*
- **payload-size** *payload-size-in-ms*



### Note

You can improve the performance of packet reordering on TDM/PWE connections by using the increasing the size of the de jitter buffer using the **de jitter-buffer** parameter.

## Examples

The following example shows how to configure CEM interface parameters:

```
Router# config t
Router(config)# class cem mycemclass
Router(config-cem-class)# de jitter-buffer 10
Router(config-cem-class)# sample-rate 32
Router(config-cem-class)# exit
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# cem class mycemclass
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	<b>dejitter-buffer</b>	Specifies the size of the dejitter buffer used for network jitter in CEM configuration mode.
	<b>idle-pattern</b>	Specifies the data pattern to transmit on the T1/E1 line when missing packets are detected on the PWE3 circuit in CEM configuration mode.
	<b>sample-rate</b>	Specifies in milliseconds the rate hardware samples the data on the attached circuit in CEM circuit configuration mode.
	<b>cem</b>	Enters circuit emulation configuration mode.

# clear gsm-abis

To clear the statistics displayed by the **show gsm-abis** commands, use the **clear gsm-abis** command in privileged EXEC mode.

**clear gsm-abis** [*serial serial-number interface-number*]

## Syntax Description

<b>serial</b>	
<i>serial-number</i>	(Optional) The serial number range is from 0 to 6.
<i>interface-number</i>	(Optional) The interface number range is from 0 to 6.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Examples

The following example shows how to clear statistics:

```
Router# clear gsm-abis serial 0/0:0
```

## Related Commands

Command	Description
<b>show gsm-abis efficiency</b>	Displays the history of GSM compression/decompression efficiency averages at intervals of 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour.
<b>show gsm-abis errors</b>	Displays error statistics counters.
<b>show gsm-abis packets</b>	Displays packet statistics counters.
<b>show gsm-abis peering [details]</b>	Displays peering status, statistics, and history.

# clear ip rtp header-compression

To clear Real-Time Transport Protocol (RTP) header compression structures and statistics, use the **clear ip rtp header-compression** privileged EXEC command.

**clear ip rtp header-compression** [*type number*]

<b>Syntax Description</b>	<i>type number</i> (Optional) Interface type and number.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Usage Guidelines</b>	If this command is used without an interface type and number, the command clears all RTP header compression structures and statistics.
-------------------------	--

<b>Examples</b>	<p>The following example clears the RTP header compression structures and statistics for multilink interface 1:</p> <pre>Router# clear ip rtp header-compression multilink1</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip rtp header-compression</b>	Enables RTP header compression.

# de jitter-buffer

To configure the size of the de jitter buffer, use the **de jitter-buffer** command in CEM configuration mode. To restore the de jitter buffer to its default size, use the **no** form of this command.

**de jitter-buffer** *size*

**no de jitter-buffer**

Syntax Description	<i>size</i>	Specifies the size of the de jitter buffer in milliseconds. The range is 4 to 500 ms; the default is 4 ms.
--------------------	-------------	--

Defaults	The default de jitter-buffer size is 4 milliseconds.
----------	--

Command Modes	CEM configuration
---------------	-------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

Examples	The following example shows how to specify the size of the de jitter buffer:
----------	--

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# de jitter-buffer 10
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	<b>cem</b>	Enters circuit emulation configuration mode.
	<b>cem class</b>	Applies the CEM interface parameters defined in the given CEM class name to the circuit.
	<b>class cem</b>	Configures CEM interface parameters in a class that's applied to CEM interfaces together in global configuration mode.

## gsm-abis congestion abate

To set the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated, use the **gsm-abis congestion abate** interface configuration command. The abatement detection level is defined as  $x$  milliseconds of continuous congestion abatement (that is, no congestion indications).

**gsm-abis congestion abate** *ms*

Syntax Description	<i>ms</i>	Sets the number of milliseconds for the abatement detection level.
--------------------	-----------	--

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows how to set the abatement detection level to 250 ms:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# gsm-abis congestion abate 250
Router(config-if)# no keepalive
```

Related Commands	Command	Description
	<b>gsm-abis congestion critical</b>	Defines the critical time slots that are exempt from suppression during congestion onset.
	<b>gsm-abis congestion enable</b>	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote router when congestion is detected.
	<b>gsm-abis congestion onset</b>	Sets the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion.
	<b>gsm-abis jitter</b>	Sets the amount of transmit jitter delay for the GSM-Abis interface.
	<b>gsm-abis local</b>	Configures the local parameters for an IP/UDP backhaul connection.
	<b>gsm-abis remote</b>	Configures the remote parameters for an IP/UDP backhaul connection.

# gsm-abis congestion critical

To define the critical time slots that are exempt from suppression during congestion onset, use the **gsm-abis congestion critical** interface configuration command. These time slots contain signaling and control information exchanged between the BSC and BTS.

**gsm-abis congestion critical** *time-slot-range*

<b>Syntax Description</b>	<i>time-slot-range</i>	Specifies a value or range of values for time slots that are exempt from suppression during congestion onset. Use a hyphen to indicate a range.
---------------------------	------------------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows how to set the time-slot range:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# gsm-abis congestion critical 2-3
Router(config-if)# no keepalive
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>gsm-abis congestion abate</b>	Sets the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated.
	<b>gsm-abis congestion enable</b>	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote router when congestion is detected.
	<b>gsm-abis congestion onset</b>	Sets the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion.
	<b>gsm-abis jitter</b>	Sets the amount of transmit jitter delay for the GSM-Abis interface.
	<b>gsm-abis local</b>	Configures the local parameters for an IP/UDP backhaul connection.
	<b>gsm-abis remote</b>	Configures the remote parameters for an IP/UDP backhaul connection.

# gsm-abis congestion enable

To enable the congestion detection algorithm, use the **gsm-abis congestion enable** interface configuration command. The congestion detection algorithm monitors the transmit jitter buffer and sends congestion indicator signals to the remote when congestion is detected. The remote router suppresses all time slots that are not defined as critical in an effort to alleviate congestion. The goal of the congestion detection algorithm is to save the *critical* time slots from loss of data.

## gsm-abis congestion enable

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.4(19)MR2	This command was introduced.

### Examples

The following example shows how to enable the congestion detection algorithm:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# no keepalive
```

### Related Commands

Command	Description
<b>gsm-abis congestion abate</b>	Sets the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated.
<b>gsm-abis congestion critical</b>	Defines the critical time slots that are exempt from suppression during congestion onset.
<b>gsm-abis congestion onset</b>	Sets the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion.
<b>gsm-abis jitter</b>	Sets the amount of transmit jitter delay for the GSM-Abis interface.
<b>gsm-abis local</b>	Configures the local parameters for an IP/UDP backhaul connection.
<b>gsm-abis remote</b>	Configures the remote parameters for an IP/UDP backhaul connection.



# gsm-abis congestion onset

To set the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion, use the **gsm-abis congestion onset** interface configuration command. The onset detection level is defined as *x* milliseconds of continuous congestion detected.

**gsm-abis congestion onset** *ms*

<b>Syntax Description</b>	<i>ms</i>	Sets the number of milliseconds for the onset detection level.
---------------------------	-----------	--

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows how to set the onset detection level at 50 ms:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# gsm-abis congestion onset 100
Router(config-if)# no keepalive
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>gsm-abis congestion abate</b>	Sets the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated.
	<b>gsm-abis congestion critical</b>	Defines the critical time slots that are exempt from suppression during congestion onset.
	<b>gsm-abis congestion enable</b>	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote router when congestion is detected.
	<b>gsm-abis jitter</b>	Sets the amount of transmit jitter delay for the GSM-Abis interface.
	<b>gsm-abis local</b>	Configures the local parameters for an IP/UDP backhaul connection.
	<b>gsm-abis remote</b>	Configures the remote parameters for an IP/UDP backhaul connection.

## gsm-abis jitter

To set the amount of transmit jitter delay for the GSM-Abis interface, use the **gsm-abis jitter** interface configuration command. If the transmit jitter is set to 4 ms, data received on the backhaul with a time equal to 0 ms will be stored in the jitter buffer and transmitted with a time equal to 4 ms. The transmit jitter buffer allows some amount of jitter in the arrival of data on the backhaul to be tolerated without introducing errors into the stream of data.

**gsm-abis jitter** *ms*

Syntax Description	<i>ms</i>	Sets the number of milliseconds for the jitter. The default value is 4 ms. Valid values are 4–500 ms.
--------------------	-----------	---

Defaults	The default jitter value is 4 ms.
----------	-----------------------------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows how to set the jitter level to 8 ms:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis jitter 8
Router(config-if)# no keepalive
```

Related Commands	Command	Description
	<b>gsm-abis congestion abate</b>	Sets the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated.
	<b>gsm-abis congestion critical</b>	Defines the critical time slots that are exempt from suppression during congestion onset.
	<b>gsm-abis congestion enable</b>	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote router when congestion is detected.
	<b>gsm-abis congestion onset</b>	Sets the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion.

Command	Description
<b>gsm-abis local</b>	Configures the local parameters for an IP/UDP backhaul connection.
<b>gsm-abis remote</b>	Configures the remote parameters for an IP/UDP backhaul connection.

# gsm-abis local

To configure the local parameters required to establish an Internet Protocol/User Data Protocol (IP/UDP) backhaul connection, use the **gsm-abis local** interface configuration command.

**gsm-abis local** [*ip-address*] [*port*]

<b>Syntax Description</b>	<i>ip-address</i>	(Optional) The IP address for the entry you want to establish.
	<i>port</i>	(Optional) The port you want to use for the entry you want to establish.
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.
<b>Examples</b>	<p>The following example shows how to configure the local parameters:</p> <pre>Router(config)# <b>interface Serial10/2.0</b> Router(config-if)# <b>encapsulation gsm-abis</b> Router(config-if)# <b>gsm-abis local 10.10.10.2 5502</b></pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>gsm-abis remote</b>	Configures the remote parameters for an IP/UDP backhaul connection.

# gsm-abis lost-recovery

This command allows you to control the speed at which the router retransmits subrate data for lost packets. This method of retransmission prevents large retransmission packets from delaying subsequent backhaul packets.

To set the retransmission rate for subrate data for the lost packets, use the **gsm-abis lost-recovery** configuration command.

**gsm-abis lost-recovery** *milliseconds*

<b>Syntax Description</b>	<i>milliseconds</i>	The retransmission rate for subrate data, in milliseconds. Range is 0-5000.
	<b>Note</b>	Any value under 40 causes the router to send all subrates at once when lost packet is indicated, effectively disabling the feature.

<b>Defaults</b>	The default setting is gsm-abis lost-recovery 1250.
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<table> <tr> <th data-bbox="386 1018 475 1047">Release</th><th data-bbox="667 1018 808 1047">Modification</th></tr> <tr> <td data-bbox="386 1056 537 1085">12.4(19)MR2</td><td data-bbox="667 1056 1013 1085">This command was introduced.</td></tr> </table>	Release	Modification	12.4(19)MR2	This command was introduced.
Release	Modification				
12.4(19)MR2	This command was introduced.				

<b>Examples</b>	The following example shows how to configure the remote parameters:
-----------------	---

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis remote 10.10.10.1 5504
Router(config)# gsm-abis lost-recovery 1250
```

<b>Related Commands</b>	<table> <tr> <th data-bbox="386 1407 493 1436">Command</th><th data-bbox="769 1407 894 1436">Description</th></tr> <tr> <td data-bbox="386 1444 623 1474">gsm-abis retransmit</td><td data-bbox="769 1444 1365 1474">Enables retransmission of a repetitive subrate sample.</td></tr> </table>	Command	Description	gsm-abis retransmit	Enables retransmission of a repetitive subrate sample.
Command	Description				
gsm-abis retransmit	Enables retransmission of a repetitive subrate sample.				

# gsm-abis remote

To configure the remote parameters required to establish an Internet Protocol/User Data Protocol (IP/UDP) backhaul connection, use the **gsm-abis remote** interface configuration command.

**gsm-abis remote** [*ip-address*] [*port*]

## Syntax Description

<i>ip-address</i>	(Optional) The IP address for the entry you want to establish.
<i>port</i>	(Optional) The port you want to use for the entry you want to establish.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Examples

The following example shows how to configure the remote parameters:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis remote 10.10.10.1 5504
```

## Related Commands

Command	Description
<b>gsm-abis local</b>	Configures the local parameters for an IP/UDP backhaul connection.

# gsm-abis retransmit

To enable retransmission of a repetitive subrate sample, use the **gsm-abis retransmit** interface configuration command. This command is useful when the latency introduced by the characteristics of the backhaul network is excessive. Examples of excessive latency include the use of satellite transmission facilities or multiple router hops on the backhaul network.

**gsm-abis retransmit** *sample-delay*

<b>Syntax Description</b>	<i>sample-delay</i>	The number of duplicate samples that must be observed before the duplicate sample is retransmitted. The delay range is 5 to 255 or 100 to 5100 ms at 20-ms intervals.
---------------------------	---------------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows how to set a retransmit delay of 100 ms:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis local 10.10.10.1 5504
Router(config-if)# gsm-abis remote 10.10.10.2 5504
Router(config-if)# gsm-abis retransmit 5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>gsm-abis local</b>	Configures the local parameters for an IP/UDP backhaul connection.
	<b>gsm-abis remote</b>	Configures the remote parameters for an IP/UDP backhaul connection.
	<b>show gsm-abis packet</b>	Displays packet statistics counters of the GSM compression/decompression.
	<b>show gsm-abis packet   include retransmit</b>	Displays packet statistics counters of the GSM compression/decompression to include the repetitive subrate samples retransmitted.

# gsm-abis set dscp

To mark a packet by setting the differential services code point (DSCP) for GSM-Abis, use the **gsm-abis set dscp** interface configuration command.

**gsm-abis set dscp** *value*



**Note**

Use this command when configuring GSM shorthaul interfaces.

Syntax Description	<i>value</i>	A number from 0 to 63 that sets the GSM-Abis DSCP value.
--------------------	--------------	--

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

## Examples

The following example shows how to mark a packet:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis local 10.10.10.1 5504
Router(config-if)# gsm-abis remote 10.10.10.2 5504
Router(config-if)# gsm-abis set dscp cs2
```



# idle-pattern

To specify the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit, use the **idle-pattern** command in CEM configuration mode. To stop sending idle pattern data, use the **no** form of this command.

**idle-pattern** [*pattern*]

**no idle-pattern**

## Syntax Description

<i>pattern</i>	(Optional) An 8-bit hexadecimal number that is transmitted as the idle pattern. T1 and E1 channels require only this argument.
----------------	--

## Defaults

For T1 or E1 channels, the default idle pattern is 0xFF.

## Command Modes

CEM circuit configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

The idle-pattern data is sent to replace the data from missing packets.

## Examples

The following example shows how to specify a data pattern:

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# idle-pattern 0x55
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<b>cem</b>	Enters circuit emulation configuration mode.
<b>cem class</b>	Applies the CEM interface parameters defined in the given CEM class name to the circuit.
<b>class cem</b>	Configures CEM interface parameters in a class that's applied to CEM interfaces together in global configuration mode.

# ima-group

To define physical links as inverse multiplexing over ATM (IMA) group members, use the **ima-group** command in interface configuration mode. When you first perform the configuration or when you change the group number, the interface is automatically disabled, moved to the new group, and then enabled. To remove the group, use the **no** form of this command.

```
ima-group group-number

no ima-group group-number
```

Syntax Description	group-number	Specifies an IMA group number from 0 to 3. IMA groups can span multiple ports on a port adapter or shared port adapter (SPA) but cannot span port adapters or SPAs.
--------------------	--------------	---

Defaults	No IMA groups are defined.
----------	----------------------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.4(19)MR2	This command was introduced.

Usage Guidelines	Use the <b>ima-group</b> interface command to configure a T1/E1 IMA port adapter interface as part of an IMA group.
------------------	---

Examples	The following example shows how to define an IMA group:
----------	---

```
Router(config)# interface ATM0/0
Router(config-if)# no ip address
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# ima-group 0
```

Related Commands	Command	Description
	interface atm	Configures an ATM interface.
	interface atm ima	Configures an ATM IMA group.
	show ima interface atm	Provides information about all configured IMA groups or a specific IMA group.

# interface atm ima

To configure an ATM IMA group and enter interface configuration mode, use the **interface atm ima** global configuration command. If the group does not exist when the command is issued, the command automatically creates the group.

**interface atm** *slot/imagroup-number*

Syntax Description	<i>slot</i>	Specifies the slot location of the ATM IMA port adapter.
	<i>group-number</i>	Specifies an IMA group number from 0 to 3. You can create up to four groups.

Defaults	The interface includes individual ATM links, but no IMA groups.
----------	---

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

Usage Guidelines	When a port is configured for IMA functionality, it no longer operates as an individual ATM link. Specifying ATM links as members of a group using the <b>ima-group</b> interface command does not enable the group. You must use the <b>interface atm slot/imagroup-number</b> command to create the group.
------------------	--

Examples	The following example shows the how to create the IMA group:
----------	--

```
Router(config)# interface ATM0/IMA0
Router(config-if)# no ip address
```

Related Commands	Command	Description
	<b>ima-group</b>	Configures the physical links as IMA group members; execute this interface configuration command for each physical link that you include in an IMA group.
	<b>ima group-id</b>	Enables the user to configure the IMA Group ID for the IMA interface.
	<b>interface atm</b>	Configures physical links for an ATM interface.
	<b>show ima interface atm</b>	Displays general and detailed information about IMA groups and the links they include.

# ip local interface

To configure the IP address of the provider edge (PE) router interface to be used as the source IP address for sending tunneled packets, use the **ip local interface** command in pseudowire-class configuration mode. To remove the IP address, use the **no** form of this command.

**ip local interface** *interface-name*

**no ip local interface** *interface-name*

## Syntax Description

<i>interface-name</i>	Name of the PE interface whose IP address is used as the source IP address for sending tunneled packets over a Layer 2 PW.
-----------------------	--

## Defaults

No IP address is configured.

## Command Modes

Pseudowire-class configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

Use the same local interface name for all pseudowire-classes configured between a pair of PE routers. It is highly recommended that you configure a loopback interface with this command. If you do not, the router chooses the “best available local address,” which could be any IP address configured on a core-facing interface. This configuration could prevent a control channel from being established.

## Examples

The following example shows how to configure the IP address of the local loopback 0 as the source IP address for sending packets through an MPLS session:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# ip local interface loopback 0
Router(config-pw-class)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<b>ima-group</b>	Configures the physical links as IMA group members, which executes the interface configuration command for each physical link included in an IMA group.
<b>ima group-id</b>	Enables the user to configure the IMA Group ID for the IMA interface.

Command	Description
<b>interface atm</b>	Configures physical links for an ATM interface.
<b>show ima interface atm</b>	Displays general and detailed information about IMA groups and the links they include.

# ip rtp header-compression

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

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

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

## Syntax Description

<b>passive</b>	(Optional) Compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed. If you do not specify the <b>passive</b> keyword, all RTP packets are compressed.
<b>iphc-format</b>	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
<b>ietf-format</b>	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used.
<b>periodic-refresh</b>	(Optional) Indicates that the compressed IP header will be refreshed periodically.

## Defaults

Disabled.

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

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

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

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

### passive Keyword

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

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

### iphc-format Keyword

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

The **iphc-format** keyword includes checking whether the destination port number is even and is in the ranges of 16,385 to 32,767 (for Cisco audio) or 49,152 to 65,535 (for Cisco video). Valid RTP packets that meet the criteria (that is, the port number is even and is within the specified range) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.



#### Note

The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

### ietf-format Keyword

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

With the **ietf-format** keyword, any even destination port number higher than 1024 can be used. Valid RTP packets that meet the criteria (that is, the port number is even and is higher than 1024) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.



#### Note

The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format** keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

### Support for Serial Lines

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

### Unicast or Multicast RTP Packets

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

### Examples

The following example enables RTP header compression on the Serial1/0 interface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip rtp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# exit
```

The following example enables RTP header compression on the Serial1/0 interface and limits the number of RTP header compression connections to 20. In this example, the optional **iphc-format** keyword of the **ip rtp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 20
Router(config-if)# exit
```

In the following example, RTP header compression is enabled on the Serial1/0 interface and the optional **periodic-refresh** keyword of the **ip rtp header-compression** command is specified:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format periodic-refresh
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# exit
```

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



# ip tcp header-compression

To enable Transmission Control Protocol (TCP) header compression, use the **ip tcp header-compression** command in interface configuration mode. To disable compression, use the **no** form of this command.

**ip tcp header-compression** [**passive**] [**iphc-format**] [**ietf-format**]

**no ip tcp header-compression** [**passive**] [**iphc-format**] [**ietf-format**]

## Syntax Description

<b>passive</b>	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the <b>passive</b> keyword, all TCP packets are compressed.
<b>iphc-format</b>	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
<b>ietf-format</b>	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used.

## Defaults

Disabled.

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

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format is as described in RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. Compressing the TCP header can speed up Telnet connections dramatically.

In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on User Datagram Protocol (UDP) packets or other headers.

### passive Keyword

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

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

#### iphc-format Keyword

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



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

#### ietf-format Keyword

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



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

### Examples

The following example sets the first serial interface for header compression with a maximum of 10 cache entries:

```
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
```

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

```
Router(config)# interface serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
```

The following example enables RTP header compression on the Serial1/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified.

```
Router(config)# interface serial1/0.0
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
```

Related Commands	Command	Description
	<b>ip tcp compression-connections</b>	Specifies the total number of TCP header compression connections that can exist on an interface.
	<b>show ip tcp header-compression</b>	Displays TCP header compression statistics.
	<b>show running-config</b>	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

# ipran-mib backhaul-notify-interval

To specify the interval used to suppress the generation of the ciscoIpRanBackHaulRcvdUtil and the ciscoIpRanBackHaulSentUtil notifications from the CISCO-IP-RAN-BACKHAUL-MIB, use the **ipran-mib backhaul-notify-interval** command in global configuration mode. To remove the interval, use the **no** form of the command.

```
ipran-mib backhaul-notify-interval interval

no ipran-mib backhaul-notify-interval interval
```

Notifications are suppressed for the number of seconds specified. Notifications are not suppressed when this keyword is set to zero. The minimum interval is 1 minute and the maximum is 15 minutes. When suppression is enabled, notifications are generated when a worse state is encountered. For example, the following transitions generate notifications:

- “acceptable” to “warning”
- “warning” to “overloaded”

Later transitions to lesser states are suppressed. For example, the following transitions do not generate notifications:

- “warning” to “acceptable”
- “overloaded” to “warning”
- “overloaded” to “acceptable”

At the end of the specified interval, a notification is generated if the current state is different from the state reported by the last notification.

Syntax Description	<i>interval</i> 60 to 900 seconds, or 0 (zero).
--------------------	---

Defaults	The default interval is 0 (notifications are not suppressed).
----------	---

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to set the notification-suppression interval:

```
Router# config t
Router(config)# ipran-mib backhaul-notify-interval 60
Router(config)# ipran-mib backhaul-notify-interval 900
Router(config)# no ipran-mib backhaul-notify-interval
Router(config)# exit
```

**Related Commands**

Command	Description
<b>ipran-mib threshold-acceptable</b>	Specifies the acceptable level of traffic.
<b>ipran-mib threshold-overloaded</b>	Specifies the amount of traffic that indicates the backhaul is overloaded.
<b>ipran-mib threshold-warning</b>	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.

# ipran-mib location

To define the location of the device, use the **ipran-mib location** command in global configuration mode. The command is also used to assist the network management system in properly displaying the topology of the system.

**ipran-mib location** {addSite | cellSite | undefined}

## Syntax Description

<b>addSite</b>	Locates the device at a BSC or RNC site.
<b>cellSite</b>	Locates the device at a BTS or Node B site.
<b>undefined</b>	Specifies an undefined location for the device.

## Defaults

The default location is cellSite.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Examples

The following example shows how to define the device location:

```
Router# config t
Router(config)# ipran-mib location aggSite
Router(config)# ipran-mib location cellSite
Router(config)# ipran-mib location undefined
Router(config)# no ipran-mib location
Router(config)# exit
```

## Related Commands

Command	Description
<b>ipran-mib snmp-access</b>	Defines the type of connectivity between the device and the network management system.

# ipran-mib snmp-access

To define the type of connectivity between the device and the network management system, use the **ipran-mib snmp-access** command in global configuration mode. The command is used to limit the amount of traffic while the network is in the process of in-band polling.

**ipran-mib snmp-access {inBand | outOfBand | undefined}**

Syntax Description	inBand	Defines in-band SNMP connectivity.
	outOfBand	Defines out-of-band SNMP connectivity.
	undefined	Specifies undefined connectivity.

Defaults	The default access type is inBand.
----------	------------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

Examples	The following example shows how to define the connectivity type:
----------	--

```
Router# config t
Router(config)# ipran-mib snmp-access inBand
Router(config)# ipran-mib snmp-access outOfBand
Router(config)# ipran-mib snmp-access undefined
Router(config)# no ipran-mib snmp-access
Router(config)# exit
```

Related Commands	Command	Description
	ipran-mib location	Defines the location of the device. It is also used to assist the network management system in properly displaying the topology of the system.

# ipran-mib threshold-acceptable

To specify a level of traffic below which the instances of the `cirbhBackHaulRcvdUtilState` and `cirbhBackHaulSentUtilState` objects are marked as “acceptable,” use the **ipran-mib threshold-acceptable** command in global configuration mode. All changes to this threshold take effect at the end of the current interval. The value for this object must be less than the values specified by the **ipran-mib threshold-warning** and **ipran-mib threshold-overloaded** commands. This parameter corresponds to the `cirbhBackHaulAcceptableThreshold` object.

**ipran-mib threshold-acceptable** [*utilization-percentage*]

<b>Syntax Description</b>	<i>utilization-percentage</i>	(Optional) Specifies the utilization threshold as a percentage. The range is 20 to 100 percent.
---------------------------	-------------------------------	---

<b>Defaults</b>	The default threshold is 60 percent.
-----------------	--------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Examples</b>	The following example shows how to set the utilization threshold:
-----------------	---

```
Router# config t
Router(config)# ipran-mib threshold-acceptable 50
Router(config)# ipran-mib threshold-acceptable 70
Router(config)# no ipran-mib threshold-acceptable
Router(config)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ipran-mib threshold-overloaded</b>	Specifies the amount of traffic that indicates the backhaul is overloaded.
	<b>ipran-mib threshold-warning</b>	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.
	<b>ipran-mib backhaul-notify-interval</b>	Specifies the interval used to suppress the generation of utilization notifications.



# ipran-mib threshold-overloaded

To specify a level of traffic where the instances of the cirbhBackHaulRcvdUtilState and cirbhBackHaulSentUtilState objects are marked as “overloaded,” use the **ipran-mib threshold-overloaded** command in global configuration mode. Changes to this threshold take effect at the end of the current interval. The value for this object must be greater than the value specified for the cirbhBackHaulAcceptableThreshold object. Also, the value for this object must be greater than or equal to the value of the cirbhBackHaulWarningThreshold object.

**ipran-mib threshold-overloaded** [*utilization-percentage*]

<b>Syntax Description</b>	<i>utilization-percentage</i> (Optional) Specifies the utilization threshold as a percentage. The range is 40 to 100 percent.
---------------------------	---

<b>Defaults</b>	The default threshold is 80 percent.
-----------------	--------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Examples</b>	The following example shows how to set the utilization threshold:
-----------------	---

```
Router# config t
Router(config)# ipran-mib threshold-overloaded 60
Router(config)# ipran-mib threshold-overloaded 80
Router(config)# no ipran-mib threshold-warning
Router(config)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ipran-mib threshold-acceptable</b>	Specifies the acceptable level of traffic.
	<b>ipran-mib backhaul-notify-interval</b>	Specifies the interval used to suppress the generation of utilization notifications.
	<b>ipran-mib threshold-warning</b>	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.

# ipran-mib threshold-warning

To specify a level of traffic where the instances of the `cirbhBackHaulRcvdUtilState` and `cirbhBackHaulSentUtilState` objects are marked as “warning,” use the **ipran-mib threshold-warning** command in global configuration mode.

All changes to this threshold take effect at the end of the current interval. The value for this object must be greater than the value specified for the **ipran-mib threshold-acceptable** command. Also, the value for this object must be less than or equal to the value of the `cirbhBackHaulOverloadedThreshold` object. This parameter corresponds to the `cirbhBackHaulWarningThreshold` object.

**ipran-mib threshold-warning** [*utilization-percentage*]

<b>Syntax Description</b>	<i>utilization-percentage</i>	(Optional) Specifies the utilization threshold as a percentage. The range is 30 to 100 percent.
---------------------------	-------------------------------	---

<b>Defaults</b>	The default threshold is 70 percent.
-----------------	--------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	12.4(19)MR2	This command was incorporated.

<b>Examples</b>	The following example shows how to set the utilization threshold:
-----------------	---

```
Router# config t
Router(config)# ipran-mib threshold-warning 60
Router(config)# ipran-mib threshold-warning 80
Router(config)# no ipran-mib threshold-warning
Router(config)# exit
```

<b>Related Commands</b>	Command	Description
	<b>ipran-mib threshold-acceptable</b>	Specifies the acceptable level of traffic.
	<b>ipran-mib threshold-overloaded</b>	Specifies the amount of traffic that indicates the backhaul is overloaded.
	<b>ipran-mib backhaul-notify-interval</b>	Specifies the interval used to suppress the generation of utilization notifications.

# keepalive

To enable keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface, use the **keepalive** command in interface configuration mode.

When the keepalive function is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. To turn off keepalive packets entirely, use the **no** form of this command.

**keepalive** [*period* [*retries*]]

**no keepalive** [*period* [*retries*]]

## Syntax Description

<i>period</i>	(Optional) Integer value in seconds, that represents the time interval between messages sent by the Cisco IOS software to ensure that a network interface is alive. The value must be greater than 0, and the default is 10.
<i>retries</i>	(Optional) Number of times that the device will continue to send keepalive packets without response before bringing the interface down. The integer value is greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value was specified previously, the default value of 5 is used.  If this command is used with a tunnel interface, then this variable specifies the number of times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down.

## Defaults

*period*: 10 seconds

*retries*: 5

If you enter the **keepalive** command with no arguments, the defaults for both arguments are used.

If you enter the **keepalive** command and the timeout (*period*) argument, the default number of retries (5) is used.

If you enter the **no keepalive** command, keepalive packets are disabled on the interface.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

---

**Usage Guidelines****Keepalive Time Interval**

You can configure the keepalive time interval, which is the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (serial and tunnel), to ensure that a network interface is alive. The interval is adjustable in 1-second increments, down to a minimum of 1 second. An interface is declared down after three update intervals have passed without receiving a keepalive packet unless the retry value is set higher.

Setting the keepalive timer to a low value is useful for quickly detecting Ethernet interface failures (such as a transceiver cable disconnecting, or cable that is not terminated).

**Line Failure**

A typical serial line failure involves losing the Carrier Detect (CD) signal. Because this sort of failure is typically noticed within a few milliseconds, adjusting the keepalive timer for quicker routing recovery is generally not useful.

**Keepalive Packets with Tunnel Interfaces**

GRE keepalive packets may be sent either from both sides of a tunnel or from just one side. If they are sent from both sides, the *period* and *retries* arguments can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

**Dropped Packets**

Because keepalive packets are treated as ordinary packets, it is possible that they will be dropped. To reduce the possibility that dropped keepalive packets will cause the tunnel interface to be taken down, increase the number of retries.

**Note**

---

When adjusting the keepalive timer for a very-low-bandwidth serial interface, large datagrams can delay the smaller keepalive packets long enough to cause the line protocol to go down. You may need to experiment to determine the best values to use for the timeout and the number of retry attempts.

---

---

**Examples**

The following example shows how to set the keepalive interval to 3 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)# keepalive 3
```

The following example shows how to set the keepalive interval to 3 seconds and the retry value to 7:

```
Router(config)# interface tunnel 1
Router(config-if)# keepalive 3 7
```

# load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. Use the **no** form of this command to revert to the default setting.

**load-interval** *seconds*

**no load-interval** *seconds*

Syntax Description	<i>seconds</i>	Length of time for which data is used to compute load statistics. Specify a value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so forth).
--------------------	----------------	---

Defaults	The default is 300 seconds (5 minutes).
----------	---

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

Usage Guidelines	<p>If you want load computations to be more reactive to short bursts of traffic, rather than averaged over 5-minute periods, you can shorten the length of time over which load averages are computed.</p> <p>If the load interval is set to 30 seconds, new data is used for load calculations over a 30-second period. This data is used to compute load statistics, including input rate in bits and packets per second, output rate in bits and packets per second, load, and reliability.</p> <p>Load data is gathered every 5 seconds. This data is used for a weighted average calculation in which more-recent load data has more weight in the computation than older load data. If the load interval is set to 30 seconds, the average is computed for the last 30 seconds of load data.</p> <p>The <b>load-interval</b> command allows you to change the default interval of 5 minutes to a shorter or longer period of time. If you change it to a shorter period of time, the input and output statistics that are displayed when you use the <b>show interface</b> command will be more current, and based on more instantaneous data, rather than reflecting a more average load over a longer period of time.</p> <p>This command is often used for dial backup purposes, to increase or decrease the likelihood of a backup interface being implemented, but it can be used on any interface.</p>
------------------	--

Examples	<p>In the following example, the default 5-minute average is set to a 30-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default 5-minute interval might trigger a dial backup for this interface that is set for a shorter, 30-second interval.</p>
----------	---

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

load-interval

Related Commands

Command	Description
show interfaces	Displays ALC information.

# match ip dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match ip dscp** class-map configuration command. To remove a specific IP DSCP value from a class map, use the **no** form of this command.

```
match ip dscp ip-dscp-value [ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value  
ip-dscp-value ip-dscp-value ip-dscp-value]
```

```
no match ip dscp ip-dscp-value [ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value  
ip-dscp-value ip-dscp-value ip-dscp-value]
```

<b>Syntax Description</b>	<i>ip-dscp-value</i>	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.
---------------------------	----------------------	---

<b>Command Modes</b>	Class-map configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Usage Guidelines</b>	Up to eight IP DSCP values can be matched in one match statement. For example, if you wanted the IP DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values), enter the <b>match ip dscp 0 1 2 3 4 5 6 7</b> command.
-------------------------	--

This command is used by the class map to identify a specific IP DSCP value marking on a packet. The *ip-dscp-value* arguments are used as markings only. The IP DSCP values have no mathematical significance. For instance, the *ip-dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with an *ip-dscp-value* of 2 is different from a packet marked with an *ip-dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Examples

The following example shows how to configure the service policy called priority55 and attach service policy priority55 to an interface. In this example, the class map called ipdscp15 evaluates all packets entering interface Fast Ethernet 0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet is treated with a priority level of 55.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config-cmap)# exit
Router(config)# policy-map priority55
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority55
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa0/0
Router(config-if)# service-policy input priority55
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip dscp	Marks the IP DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.



# mpls ip

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths for a specified interface, use the **mpls ip** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**mpls ip**

**no mpls ip**

## Syntax Description

This command has no arguments or keywords.

## Defaults

MPLS forwarding of IPv4 packets along normally routed paths for the interface is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching has been enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the **no** form of the command does not affect the sending of labeled packets through any LSP tunnels that might use the interface.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) beginning at, terminating at, or passing through the interface.

## Examples

The following example shows that label switching is enabled on the specified Ethernet interface:

```
Router# config t
Router(config)# configure terminal
Router(config-if)# interface Ethernet 0/2
Router(config-if)# mpls ip
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	<b>mpls ldp maxhops</b>	Limits the number of hops permitted in an LSP established by the downstream-on-demand method of label distribution.
	<b>show mpls interfaces</b>	Displays information about one or more interfaces that have been configured for label switching.

# network-clock-select hold\_timeout

The **network-clock-select hold\_timeout** command specifies how long the router waits before reevaluating the network clock entry. To remove a **network-clock-select hold\_timeout** configuration, use the **no** form of this command.

**network-clock-select hold\_timeout** {*timeout* | **infinite**}

**no network-clock-select hold\_timeout** {*timeout* | **infinite**}

## Syntax Description

<i>timeout</i>	A value in seconds that specifies how long the router waits before reevaluating the network clock entry. Valid values are a number from 0–86400.
<b>infinite</b>	Specifies an infinite holdover.

## Defaults

The default setting is **network-clock-select hold\_timeout infinite**.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t  
Router(config)# network-clock-select hold_timeout 2000  
Router(config)# exit
```

## Related Commands

Command	Description
<b>set network-clock-select force-reselect</b>	Forces the router to re-select the network clock.

# network-clock-select input-stratum4

The **network-clock-select input-stratum4** command allows you to downgrade a clock source from Stratum3 to Stratum 4. To configure a clock source as Stratum 3, use the **no** form of this command.

**network-clock-select input-stratum4**

**no network-clock-select input-stratum4**

## Defaults

The default setting is for onboard E1/T1 ports is Stratum 3; the default setting for E1/T1 HWIC ports is Stratum 4.



**Note**

You cannot configure E1/T1 HWIC ports as Stratum3.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock-select input-stratum4
Router(config)# exit
```

## Related Commands

Command	Description
<b>set network-clock-select force-reselect</b>	Forces the router to re-select the network clock.

# network-clock-select mode

The **network-clock-select mode** command specifies the router switching mode. To remove a **network-clock-select mode** configuration, use the **no** form of this command.

**network-clock-select mode {revert | nonrevert}**

**no network-clock-select mode {revert | nonrevert}**

## Syntax Description

<b>nonrevert</b>	Sets the network clock to non-revertive mode.
<b>revert</b>	Sets the network clock to revertive mode.

## Defaults

The default setting is **network-clock-select mode nonrevert**.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t  
Router(config)# network-clock-select mode revert  
Router(config)# exit
```

## Related Commands

Command	Description
<b>set network-clock-select force-reselect</b>	Forces the router to re-select the network clock.

# network-clock-select priority

The **network-clock-select** command names a source to provide timing for the network clock and to specify the selection priority for the clock source. To remove a network-clock-select configuration, use the **no** form of this command.

**network-clock-select** *priority* {bits | synce {port} | packet\_timing} {E1 | T1 slot/port}

**no network-clock-select** *priority* {bits | synce {port} | packet\_timing} {E1 | T1 slot/port}

## Syntax Description

<i>priority</i>	A numeric value from 1–22 that specifies the priority of the clock source.
<b>bits</b>	Specifies timing from a BITS port clock.
<b>synce</b>	Specifies timing using synchronous Ethernet.
<b>port</b>	Specifies the port on which synchronous Ethernet is enabled.
<b>packet_timing</b>	Enables packet timing using the RTM module.
<b>E1</b>	Specifies clocking via an E1 interface.
<b>T1</b>	Specifies clocking via a T1 interface.
<i>slot/port</i>	Specifies the slot and port of the interface used for timing.

## Defaults

There is no default setting.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock-select 1 packet_timing
Router(config)# exit
```

## Related Commands

Command	Description
<b>set network-clock-select force-reselect</b>	Forces the router to re-select the network clock.

# payload-size

Specifies the size of the payload for packets on a structured CEM channel.

**payload-size** [*payload-size*]

Syntax Description	<i>payload-size</i>	Specifies the size of the payload for packets on a structured CEM channel. Valid values are 32–512. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256 bytes.
	<b>Note</b>	The payload size must be a multiple of the number of timeslots for the CEM channel.
		The default payload size is calculated as follows: 8 x number of timeslots x 1 ms packetization delay

Defaults	The default payload size for a structured CEM channel depends on the number of timeslots that constitute the channel. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256 bytes.
----------	--

Command Modes	CEM circuit configuration
---------------	---------------------------

Command History	Release	Modification
	12.4(19)MR2	This command was introduced.

Usage Guidelines	The Cisco MWR 2941-DC only supports a payload size of 486 (625 packets per second) or 243 (1250 packets per second).
------------------	--

Examples	The following example shows how to specify a sample rate:
----------	---

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# payload-size 256
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	<b>dejitter-buffer</b>	Configures the size of the dejitter buffer on a CEM channel.
	<b>idle-pattern</b>	Specifies the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit.



# pseudowire-class

To specify the name of a Layer 2 pseudowire-class and enter pseudowire-class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

**pseudowire-class** *pw-class-name*

**no pseudowire-class** *pw-class-name*

## Syntax Description

<i>pw-class-name</i>	The name of a Layer 2 pseudowire-class. If you want to configure more than one pseudowire class, define a class name using the <i>pw-class-name</i> parameter.
----------------------	--

## Defaults

No pseudowire-class is defined.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

The **pseudowire-class** command configures a pseudowire-class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire-class includes the following configuration settings:

- Data encapsulation type
- Control protocol
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

The local interface name for each pseudowire class configured between a pair of PE routers can be the same or different.

After entering the **pseudowire-class** command, the router switches to pseudowire-class configuration mode where PW settings can be configured.

## Examples

The following example shows how to enter pseudowire-class configuration mode to configure a PW configuration template named “ether-pw”:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# exit
```

**Related Commands**

Command	Description
<b>pseudowire</b>	Binds an attachment circuit to a Layer 2 PW for an xconnect service.
<b>xconnect</b>	Binds an attachment circuit to an Layer 2 PW for an xconnect service and then enters xconnect configuration mode.

# ptp announce

Sets interval and timeout values for PTP announcement packets.

**ptp announce interval** *interval-value* **timeout** *timeout-value*

**no ptp announce interval** *interval-value* **timeout** *timeout-value*

Syntax Description	interval	<p>Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows:</p> <ul style="list-style-type: none"> <li>4—1 packet every 16 seconds</li> <li>3—1 packet every 8 seconds</li> <li>2—1 packet every 4 seconds</li> <li>1—1 packet every 2 seconds</li> <li>0—1 packet every second</li> <li>-1—1 packet every 1/2 second, or 2 packets per second</li> <li>-2—1 packet every 1/4 second, or 4 packets per second</li> <li>-3—1 packet every 1/8 second, or 8 packets per second</li> <li>-4—1 packet every 1/16 seconds, or 16 packets per second.</li> <li>-5—1 packet every 1/32 seconds, or 32 packets per second.</li> <li>-6—1 packet every 1/64 seconds, or 64 packets per second.</li> </ul> <p>The recommended value is -6.</p>
	timeout	<p>Specifies the number of PTP announcement intervals before the session times out. Valid values are 2–10.</p>

## Defaults

The default interval value is 1. The default timeout value is 3.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Usage Guidelines

The recommended interval value is -6.

## Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp announce interval 3
```

## ■ ptp announce

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

**Related Commands**

Command	Description
<a href="#">ptp enable</a>	Enables PTP mode on an interface.

# ptp clock-source

Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode.

**ptp clock-source** *clock-ip-address*

**no ptp clock-source** *clock-ip-address*

## Syntax Description

<b>clock-ip-address</b>	The IP address of the clock source.
-------------------------	-------------------------------------

## Defaults

The default setting is **no ptp clock-source**.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Examples

The following example shows how to configure a PTP clock source:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp clock-source 192.168.1.1
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<a href="#">ptp enable</a>	Enables PTP mode on an interface.
<a href="#">ptp mode</a>	Specifies the PTP mode.
<a href="#">ptp slave</a>	Sets an interface to slave clock mode for PTP clocking.

# ptp clock-destination

Specifies the IP address of a clock destination. This command applies only when the router is in PTP master unicast mode.

**ptp clock-destination** *clock-ip-address*

**no ptp clock-destination** *clock-ip-address*

<b>Syntax Description</b>	<i>clock-ip-address</i> The IP address of the clock destination.
---------------------------	--

<b>Defaults</b>	There is no default setting.
-----------------	------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was introduced.

<b>Usage Guidelines</b>	If the router is set to ptp master unicast, you can only configure a single destination. If the router is set to ptp master unicast negotiation, you can configure up to 128 clock destinations.
-------------------------	--

<b>Examples</b>	The following example shows how to configure a PTP announcement:
-----------------	--

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp clock-destination 192.168.1.2
Router(config-if)# exit
Router(config)# exit
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">ptp enable</a>	Enables PTP mode on an interface.
	<a href="#">ptp master</a>	Sets an interface in master clock mode for PTP clocking
	<a href="#">ptp mode</a>	Specifies the PTP mode.

# ptp delay-req

Specifies the delay request interval, the time recommended to member devices to send delay request messages when an interface is in PTP master mode.

**ptp delay-req interval** *interval-value*

**no ptp delay-req interval** *interval-value*

Syntax Description	interval	Specifies the interval for delay request messages. The intervals are set using log base 2 values, as follows:
		4—1 packet every 16 seconds
		3—1 packet every 8 seconds
		2—1 packet every 4 seconds
		1—1 packet every 2 seconds
		0—1 packet every second
		-1—1 packet every 1/2 second, or 2 packets per second
		-2—1 packet every 1/4 second, or 4 packets per second
		-3—1 packet every 1/8 second, or 8 packets per second
		-4—1 packet every 1/16 seconds, or 16 packets per second.
		-5—1 packet every 1/32 seconds, or 32 packets per second.
		-6—1 packet every 1/64 seconds, or 64 packets per second.
		The recommended value is -6.

**Defaults** The default setting is 0.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.4(19)MR2	This command was introduced.

**Usage Guidelines** The recommended interval value is -6.

**Examples** The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp delay-req interval -4
Router(config-if)# exit
```

```
Router(config)# exit
```

Related Commands	Command	Description
	<a href="#">ptp enable</a>	Enables PTP mode on an interface.
	<a href="#">ptp master</a>	Sets an interface in master clock mode for PTP clocking
	<a href="#">ptp mode</a>	Specifies the PTP mode.



# ptp domain

PTP domains allow you to use multiple independent PTP clocking subdomains on a single network. Use this command to specify the PTP domain number that the router uses.

**ptp domain** *domain-number*

**no ptp domain** *domain-number*

## Syntax Description

<i>domain-number</i>	The PTP domain that the router applies to PTP traffic. Valid values are from 0–127.
----------------------	---

## Defaults

The default setting is **ptp domain 0**.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Examples

The following example shows how to set the ptp domain:

```
Router# config t
Router# ptp domain 88
Router(config)# exit
```

## Related Commands

Command	Description
<a href="#">ptp enable</a>	Enables PTP mode on an interface.
<a href="#">ptp mode</a>	Specifies the PTP mode.

# ptp enable

Enables PTP mode on an interface.

**ptp enable**

**no ptp enable**

**Defaults** PTP is disabled by default.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.4(19)MR2	This command was introduced.

**Examples** The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp enable
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	<a href="#">ptp master</a>	Sets an interface in master clock mode for PTP clocking
	<a href="#">ptp mode</a>	Specifies the PTP mode.
	<a href="#">ptp slave</a>	Sets an interface to slave clock mode for PTP clocking.

# ptp master

Sets an interface in master clock mode for PTP clocking. To enable ordinary master clock mode, use the **ptp master** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**ptp master** multicast {*unicast* | **unicast negotiation**}

**no ptp master** multicast {*unicast* | **unicast negotiation**}

## Syntax Description

<b>multicast</b>	Sets the interface to use multicast mode for PTP clocking.
<b>unicast</b>	Sets the interface to use unicast mode for PTP clock.
	<b>Note</b> If the router is set to ptp master unicast, you can only configure a single destination.
<b>unicast negotiation</b>	Sets the interface to negotiate unicast mode for PTP clocking.
	<b>Note</b> If the router is set to ptp master unicast negotiation, you can configure up to 128 clock destinations.

## Defaults

There is no default setting.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Usage Guidelines

For unicast and unicast negotiation, you must configure the ip address of the remote slave using the **ptp clock-destination** command before enabling PTP.

## Examples

The following example shows how to enable ptp master multicast mode:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp master multicast
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<a href="#">ptp clock-destination</a>	Specifies the IP address of a clock destination when the router is in PTP master mode.
<a href="#">ptp enable</a>	Enables PTP mode on an interface.
<a href="#">ptp mode</a>	Specifies the PTP mode.

# ptp mode

Specifies the PTP mode.

**ptp mode [ordinary]**

**no ptp mode [ordinary]**



## Note

The Cisco MWR 2941-DC does not currently support other PTP modes such as boundary or transport mode.

## Syntax Description

<b>ordinary</b>	Sets the interface to PTP clocking mode to ordinary.
-----------------	--

## Defaults

The default setting is **ptp mode ordinary**.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Examples

The following example shows how to enable ptp mode:

```
Router# config t
Router(config)# ptp mode ordinary
Router(config)# exit
```

## Related Commands

Command	Description
<a href="#">ptp enable</a>	Enables PTP mode on an interface.
<a href="#">ptp master</a>	Sets an interface in master clock mode for PTP clocking
<a href="#">ptp slave</a>	Sets an interface to slave clock mode for PTP clocking.

# ptp priority1

Sets the preference level for a clock; slave devices use the priority1 value when selecting a master clock. The priority1 value is considered above all other clock attributes. Use the following commands to set the ptp priority1 value.

**ptp priority1** *priorityvalue*

**no ptp priority1** *priorityvalue*

## Syntax Description

<i>priorityvalue</i>	Valid values are from 0–255. The default value is 128.
----------------------	--

## Defaults

The default value is 128.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Examples

The following example shows how to enable ptp priority1 value:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp priority1 128
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<a href="#">ptp priority2</a>	Sets the PTP priority2 value.

# ptp priority2

Sets a secondary preference level for a clock; slave devices use the priority2 value when selecting a master clock. The priority2 value is considered only when the router is unable to use priority2 and other clock attributes to select a clock. Use the following commands to set the ptp priority2 value.

```
ptp priority2 priorityvalue
no ptp priority2 priorityvalue
```

Syntax Description	<p><i>priorityvalue</i> Valid values are from 0–255. The default value is 128.</p>	
Defaults	<p>The default value is 128.</p>	
Command Modes	<p>Interface configuration</p>	
Command History	Release	Modification
	12.4(19)MR2	This command was introduced.
Examples	<p>The following example shows how to configure the ptp priority2 value:</p> <pre>Router# config t Router# interface Vlan10 Router(config-if)# ptp priority2 128 Router(config-if)# exit Router(config)# exit</pre>	
Related Commands	Command	Description
	<a href="#">ptp priority1</a>	Sets the PTP priority1 value.

# ptp slave

Sets an interface to slave clock mode for PTP clocking. To enable ordinary slave clock mode, use the **ptp slave** command in interface configuration mode. To disable this feature, use the feature, use the **no** form of this command.

**ptp slave {multicast | unicast | unicast negotiation}**

**no ptp slave {multicast | unicast | unicast negotiation}**

## Syntax Description

<b>multicast</b>	Sets the interface to use multicast mode for PTP clocking.
<b>unicast</b>	Sets the interface to use unicast mode for PTP clocking.
<b>unicast negotiation</b>	Sets the interface to negotiate unicast mode for PTP clocking.

## Defaults

There is no default setting.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Usage Guidelines

You must configure the IP address of the remote timing device before enabling PTP.

## Examples

The following example shows how to enable ptp slave multicast mode:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp slave multicast
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<a href="#">ptp clock-source</a>	Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode.
<a href="#">ptp enable</a>	Enables PTP mode on an interface.
<a href="#">ptp mode</a>	Specifies the PTP mode.

# ptp sync interval

Defines the interval that the router uses to send PTP synchronization messages.

**ptp sync interval** *interval-value*

**no ptp sync interval** *interval-value*

Syntax Description	<i>interval-value</i>	Specifies the interval at which the router sends announcement packets. The intervals are set using log base 2 values, as follows:  4—1 packet every 16 seconds 3—1 packet every 8 seconds 2—1 packet every 4 seconds 1—1 packet every 2 seconds 0—1 packet every second -1—1 packet every 1/2 second, or 2 packets per second -2—1 packet every 1/4 second, or 4 packets per second -3—1 packet every 1/8 second, or 8 packets per second -4—1 packet every 1/16 seconds, or 16 packets per second. -5—1 packet every 1/32 seconds, or 32 packets per second. -6—1 packet every 1/64 seconds, or 64 packets per second.  The recommended value is -6.
--------------------	-----------------------	---

Defaults	There is no default setting.
----------	------------------------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.4(19)MR2</td><td>This command was introduced.</td></tr></table>	Release	Modification	12.4(19)MR2	This command was introduced.
Release	Modification				
12.4(19)MR2	This command was introduced.				

Usage Guidelines	We do not recommend that you alter the default value for the <b>limit</b> parameter.
------------------	--

Examples	<p>The following example shows how to configure a PTP announcement:</p> <pre>Router# config t Router(config)# interface vlan 10 Router(config-if)# ptp sync interval -4 Router(config-if)# exit Router(config)# exit</pre>
----------	--



**Related Commands**

Command	Description
<a href="#">ptp sync limit</a>	Defines the offset values that the router uses to send PTP synchronization messages.

# ptp sync limit

Defines the offset values that the router uses to send PTP synchronization messages.

**ptp sync limit** *limit-value*

**no ptp sync limit** *limit-value*

## Syntax Description

<i>limit-value</i>	Specifies the maximum clock offset value before PTP attempts to resynchronize. Values are in nanoseconds; the default value is 8000.
--------------------	--

## Defaults

The default value is 8000.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Usage Guidelines

We do not recommend that you alter the default value for the **limit** parameter unless suggested by Cisco support.

## Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp sync limit 8000
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<a href="#">ptp sync interval</a>	Defines the interval that the router uses to send PTP synchronization messages.

# pw-pvc

To configure PVC mapping or rewrite the PW configured for a PVC, use the **pw-pvc** command. This command specifies the PW-side VPI/VCI value to be used inside the PW packet payload in sending and receiving PW packets for a specified PVC.

**pw-pvc** *pw-vpi/pw-vci*

Syntax Description	<i>pw-vpi</i>	Pseudowire-side vpi value
	<i>pw-vci</i>	Pseudowire-side vci value

**Defaults** The PW-side VPI/VCI value is the same as the attachment circuit-side VPI/VCI value.

**Command Modes** l2transport VC

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows how to use the **pw-pvc** command:

```
Router# config t
Router(config-if)# pvc 0/40 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aa10
Router(config-if-atm-l2trans-pvc)# pw-pvc 1/40
Router(config-if-atm-l2trans-pvc)# xconnect 1.1.1.1 40 encapsulation mpls
Router(config-if-atm-l2trans-pvc-xconn)# exit
Router(config-if-atm-l2trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	<b>xconnect</b>	Binds an attachment circuit to a PW in one of the supported configuration modes.

# recovered-clock slave

To configure out-of-band clock recovery, use the **recovered-clock slave** command. This command automatically creates a virtual-cem interface. To access the virtual-cem interface, use the command **interface virtual-cem 0/24**. To disable this feature, use the feature, use the **no** form of this command.

- recovered-clock slave**
- no recovered-clock slave**

Defaults	There is no default setting.				
Command Modes	Global configuration				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.4(19)MR2</td><td>This command was introduced.</td></tr> </table>	Release	Modification	12.4(19)MR2	This command was introduced.
Release	Modification				
12.4(19)MR2	This command was introduced.				
Examples	<p>The following example shows how to use the <b>recovered-clock slave</b> command and how to configure the virtual-cem interface:</p> <pre> Router# config t Router(config)# recovered-clock slave Router(config-if)# interface virtual-cem 0/24 Router(config-if)# payload-size 486 Router(config-if)# cem 0 Router(config-if)# xconnect 10.10.10.2 7600 encaps mpls Router(config-if)# exit Router(config)# exit </pre>				
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td><b>recovered-clock recovered</b></td><td>Configures adaptive clock recovery.</td></tr> </table>	Command	Description	<b>recovered-clock recovered</b>	Configures adaptive clock recovery.
Command	Description				
<b>recovered-clock recovered</b>	Configures adaptive clock recovery.				

# recovered-clock recovered

The **recovered-clock recovered** command allows you to configure in-band pseudowire-based active clock recovery on a CEM interface. To disable this feature, use the **no** form of this command.

**recovered-clock recovered adaptive cem** *subslot-number port-number cem-group-number*

**no recovered-clock recovered adaptive cem** *subslot-number port-number cem-group-number*

## Syntax Description

<b>adaptive</b>	Specifies the clock recovery type.
<b>cem</b>	Specifies the Circuit emulation (CEM) interface for the recovered clock.
<i>subslot-number</i>	The subslot of the CEM interface for the recovered clock.
<i>port-number</i>	The port number of the CEM interface for the recovered clock.
<i>cem-group-number</i>	The CEM group to which the clock applies.

## Defaults

There is no default setting.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was introduced.

## Usage Guidelines

For more information about adaptive clock recovery, see [Configuring Network Clocking Support, page 4-6](#).

## Examples

The following example shows how to use the **recovered-clock recovered** command:

```
Router# config t
Router(config)# recovered-clock recovered adaptive cem 0 0 0
Router(config)# exit
```

## Related Commands

Command	Description
<b>recovered-clock slave</b>	Allows you to configure out-of-band clock recovery,

# set network-clocks

This command causes the router to reselect a network clock; the router selects a new clock based on clock priority.

**set network-clock-select [force-reselect | next-select]**

<b>Syntax Description</b>	<b>force-reselect</b>	Forces the router to select a new network clock.
	<b>next-select</b>	Forces the router to select the next available network clock.

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was introduced.

<b>Examples</b>	The following example shows how to use the set network-clock-select force-reselect command:	
	Router# <b>set network-clock-select force-reselect</b>	

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show network-clocks</b>	Displays information about all clocks configured on the router.

# show atm cell-packing

To display cell packing information for the Layer 2 attachment circuits (ACs) configured on your system, use the **show atm cell-packing** command in privileged EXEC mode.

**show atm cell-packing**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows output from the **show atm cell-packing** command:

```
Router# show atm cell-packing
```

		avg #		avg #		
Circuit		local	cells/pkt	negotiated	cells/pkt	MCPT
Type		MNCP	rcvd	MNCP	sent	(us)
ATM0/2/0/1.200	vc 1/200	1	0	1	0	50
ATM0/2/0/1.300	vc 1/300	1	0	1	0	50

Related Commands	Command	Description
	<b>cell-packing</b>	Packs multiple ATM cells into each MPLS or L2TPv3 packet.
	<b>atm cell-packing</b>	Packs multiple ATM cells into each MPLS or L2TPv3 packet.

# show cem circuit

To display a summary of CEM circuits, use the **show cem circuit** command in privileged EXEC mode.

**show cem circuit** [*cem-id*]

Syntax Description	<i>cem-id</i>	(Optional) Identifies the circuit configured with the <b>cem-group</b> command.
--------------------	---------------	---

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
GI	12.4(12)MR2	This command was introduced.

## Examples

The following examples show the output generated by this command:

```
Router# show cem circuit
CEM Int.      ID   Ctrlr   Admin   Circuit   AC
-----
CEM0/0        0   UP     UP     Enabled   UP
CEM0/1        1   UP     UP     Enabled   UP
CEM0/2        2   UP     UP     Enabled   UP
CEM0/3        3   UP     UP     Enabled   UP
CEM0/4        4   UP     UP     Enabled   UP
CEM0/5        5   UP     UP     Enabled   UP

Router# show cem circuit 5

CEM0/5, ID: 5, Line: UP, Admin: UP, Ckt: Enabled
Controller state: up
Idle Pattern: 0xFF, Idle cas: 0x8
Dejitter: 4, Sample Rate: 1, Payload Size: 192
Framing: Framed, (DS0 channels: 1-24)
CEM Defects Set
None

Signalling: No CAS
RTP: No RTP

Ingress Pkts:    527521938      Dropped:          0
Egress Pkts:    527521938      Dropped:          0

CEM Counter Details
Input Errors:    0              Output Errors:    0
Pkts Missing:    0              Pkts Reordered:   0
Misorder Drops:  0              JitterBuf Underrun: 0
Error Sec:       0              Severly Errored Sec: 0
Unavailable Sec: 0              Failure Counts:    0
Pkts Malformed:  0
```



Related Commands	Command	Description
	show cem circuit detail	Displays detailed information about all CEM circuits.
	show cem platform	Displays platform-specific error counters for all CEM circuits.
	show cem platform errors	Displays platform-specific error counters for all CEM circuits.

# show cem platform

To display platform-specific error counters for all CEM circuits, use the **show cem platform** command in privileged EXEC mode.

```
show cem platform [interface]
```

Syntax Description	interface	(Optional) Identifies the CEM interface (for example, CEM0/1).
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.4(12)MR2	This command was introduced.

**Examples** The following examples show the output generated by this command:

```
Router# show cem platform
CEM0/0 errors:
  net2cem_drops ===== 50/527658758
  net2cem_drops_underflow === 26
  net2cem_drops_overflow ==== 24
  Last cleared 6d02h
CEM0/1 errors:
  net2cem_drops ===== 50/527658759
  net2cem_drops_underflow === 25
  net2cem_drops_overflow ==== 25
  Last cleared 6d02h
CEM0/2 errors:
  net2cem_drops ===== 2/526990836
  net2cem_drops_overflow ==== 2
  Last cleared never
CEM0/3 errors:
  net2cem_drops ===== 1/526982274
  net2cem_drops_overflow ==== 1
  Last cleared never
CEM0/4 errors:
  net2cem_drops ===== 51/527658758
  net2cem_drops_underflow === 26
  net2cem_drops_overflow ==== 25
  Last cleared 6d02h
CEM0/5 errors:
  net2cem_drops ===== 48/527660498
  net2cem_drops_underflow === 24
  net2cem_drops_overflow ==== 24
  Last cleared 6d02h

Router# show cem platform cem0/1
CEM0/1 errors:
  net2cem_drops ===== 50/527678398
  net2cem_drops_underflow === 25
  net2cem_drops_overflow ==== 25
  Last cleared 6d02h
```

Related Commands	Command	Description
	show cem circuit	Displays a summary of CEM circuits.
	show cem circuit detail	Displays detailed information about all CEM circuits.
	show cem platform errors	Displays platform-specific error counters for all CEM circuits.

# show connection

To display the status of interworking connections, use the **show connection** command in privileged EXEC mode.

```
show connection [all | element | id ID | name name | port port]
```

Syntax Description	<b>all</b>	(Optional) Displays information about all interworking connections.
	<i>element</i>	(Optional) Displays information about the specified connection element.
	<b>id</b> <i>ID</i>	(Optional) Displays information about the specified connection identifier.
	<b>name</b> <i>name</i>	(Optional) Displays information about the specified connection name.
	<b>port</b> <i>port</i>	(Optional) Displays information about all connections on an interface. (In Cisco IOS Release 12.0S, only ATM, serial, and Fast Ethernet connections are shown.)

Command Modes	Privileged EXEC
---------------	-----------------

Command History	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows the local interworking connections on a router:

```
Router# show connection
ID   Name                Segment 1                Segment 2                State
=====
1    conn1               ATM 1/0/0 AAL5 0/100    ATM 2/0/0 AAL5 0/100    UP
2    conn2               ATM 2/0/0 AAL5 0/300    Serial0/1 16             UP
3    conn3               ATM 2/0/0 AAL5 0/400    FA 0/0.1 10              UP
4    conn4               ATM 1/0/0 CELL 0/500    ATM 2/0/0 CELL 0/500    UP
5    conn5               ATM 1/0/0 CELL 100      ATM 2/0/0 CELL 100      UP
```

Table A-1 describes the significant fields shown in the display.

**Table A-1** *show connection Field Descriptions*

Field	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.
Segment 1 Segment 2	Information about the interworking segments, including: <ul style="list-style-type: none"> <li>Interface name and number.</li> <li>Segment state, interface name and number, and channel ID. Segment state displays nothing if the segment state is UP, “-” if the segment state is DOWN, and “***Card Removed***” if the segment state is DETACHED.</li> <li>Type of encapsulation (if any) assigned to the interface.</li> <li>Permanent virtual circuit (PVC) assigned to the ATM interface, data-link connection identifier (DLCI) assigned to the serial interface, or VLAN ID assigned to the Ethernet interface.</li> </ul>
State or Status	Status of the connection, which is one of the following: INVALID, UP, ADMIN UP, ADMIN DOWN, OPER DOWN, COMING UP, NOT VERIFIED, ERR.

#### Related Commands

Command	Description
<b>connect (L2VPN local switching)</b>	Connects two different or similar interfaces on a router.
<b>show atm pvc</b>	Displays the status of ATM PVCs and SVCs.
<b>show frame-relay pvc</b>	Displays the status of Frame Relay interfaces.

# show controller

Use the **show controller** command to display the status of an interface.

```
show controller {ATM | Async | BITS | CEM | E1 | GigabitEthernet | J1 | T1 | RTM} slot / port
```

Syntax Description	ATM	Displays the status of the ATM controller.
	Async	Displays the status of the async controller.
	BITS	Displays the status of the BITS controller.
	CEM	Displays the status of the CEM controller.
	E1	Displays the status of the E1 controller.
	GigabitEthernet	Displays the status of the Gigabit Ethernet controller.
	J1	Displays the status of the J1 controller.
	T1	Displays the status of the T1 controller.
	RTM	Displays the status of the RTM controller.
	slot	The slot number of the interface.
	port	The port number of the interface.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

## Examples

```
Router# show controller e1 0/2
E1 0/2 is up.
  Applique type is Channelized E1 - balanced
  No alarms detected.
  alarm-trigger is not set
  Version info Firmware: 20050421, FPGA: 13, spm_count = 0
  Daughter card FPGA version: 0x16, source: Bundled
  Framing is NO-CRC4, Line Code is HDB3, Clock Source is Line.
  CRC Threshold is 320. Reported from firmware is 320.
  VWIC relays are closed
  Link noise monitor disabled
  Data in current interval (330 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    243 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
```

  
Note

The last line of the example shows 243 Slip Secs, indicating a possible clocking issue.

## Related Commands

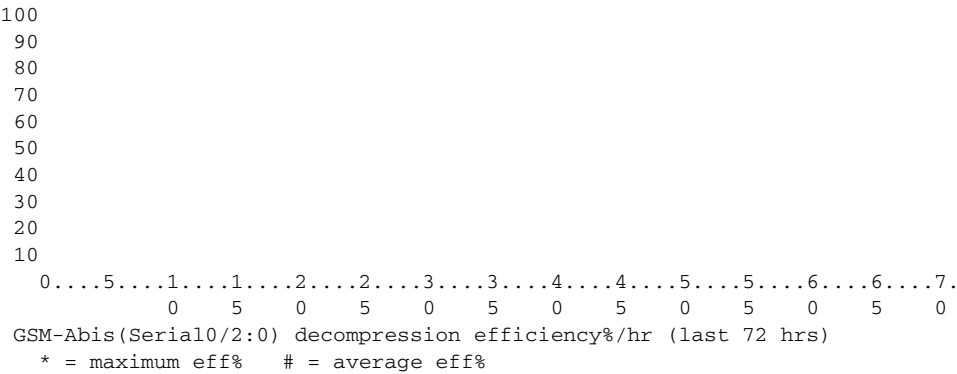
Command	Description
<b>show atm pvc</b>	Displays the status of ATM PVCs and SVCs.
<b>show frame-relay pvc</b>	Displays the status of Frame Relay interfaces.

To display a history of the GSM compression/decompression efficiency averages at intervals of 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour, use the **show gsm-abis efficiency** command in privileged EXEC mode. Efficiency is defined as the percentage of bandwidth savings obtained by using the compression/decompression algorithm to suppress GSM data.



Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide

show gsm-abis efficiency



Related Commands	Command	Description
	clear gsm-abis	Clears the statistics displayed.

# show gsm-abis errors

To display error statistics counters of GSM compression/decompression, use the **show gsm-abis errors** command in privileged EXEC mode.

## show gsm-abis errors

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows the output generated by this command:

```
Router# show gsm-abis errors
GSM-Abis(Serial0/2:0): backhaul_rxLostPakInd ===== 1/431956
GSM-Abis(Serial0/2:0): backhaul_txLostPakInd ===== 1/432539
GSM-Abis(Serial0/2:0): backhaul_missedPaks ===== 654/431956
GSM-Abis(Serial0/2:0): backhaul_latePaks ===== 591
GSM-Abis(Serial0/2:0): backhaul_lostPaks ===== 1
GSM-Abis(Serial0/2:0): backhaul_txReset ===== 33
GSM-Abis(Serial0/2:0): backhaul_overrun ===== 29
GSM-Abis(Serial0/2:0): compression_failures ===== 39661
GSM-Abis(Serial0/2:0): backhaul_congestion_drops ===== 39661
GSM-Abis(Serial0/2:0): backhaul_congestion_events ===== 1
GSM-Abis(Serial0/2:0): backhaul_congestion_duration(sec) == 80
GSM-Abis(Serial0/2:0): backhaul_congestion_bytes ===== 16498976
Last cleared 00:14:24
```

Table A-2 describes the significant fields shown in the display.

**Table A-2** *show gsm-abis errors Field Descriptions*

Field	Description
tx_gsmPak_failures	Send GSM-Abis packet failed.
txPctl_no_memory	No particles available (for example, getparticle() failure).
backhaul_peer_not_ready	Backhaul peer not ready for input.
backhaul_peer_not_active	Backhaul peer is not active. Backhaul peer is marked active when first. Backhaul peer is received from peer.
backhaul_invalid_pak	Received backhaulPak is invalid. Returns errorCode to identify reason.
backhaul_rxLostPakInd	Receive backhaul_lostPak indicator.

**Table A-2** *show gsm-abis errors Field Descriptions (continued)*

Field	Description
backhaul_txLostPakInd	Transmit backhaul_lostPak indicator.
backhaul_missedPak	Received backhaulPak is missed or dropped.
backhaul_latePaks	No backhaul packet arrived in time to fill txParticles with data (backhaul packet was lost or late).
backhaul_lostPaks	Backhaul packet was lost.
backhaul_txPctl_no_memory	No particles available (for example, getparticle () failure).
backhaul_txReset	Packets lost due to txBufferRing reset.
decompression_failures	Decompression of input backhaulPak failed.
compression_failures	Compression of input GSM packet failed.
no-backhaul_pak_available	No memory for backhaulPak buffer.
no-backhaul_interface	Could not find an output interface that corresponds to configured remote IP address.
backhaul_interface_down	Interface used for backhaul is not active.
backhaul_encap_failures	The pak-encap failed.
backhaul_qos_classify_drops	QoS classification drops.
rxInterrupt_failures	Count number of Abis packets missed because of unexpected rxInterrupt.
abis_late	GSM-Abis rxInterrupt arrived too late.
abis_early	GSM-Abis rxInterrupt arrived too early.

**Related Commands**

Command	Description
<b>clear gsm-abis</b>	Clears the statistics displayed.

# show gsm-abis packets

To display packet statistics counters of GSM compression/decompression, use the **show gsm-abis packets** command in privileged EXEC mode. Include the **include retransmit** keyword to see the repetitive substrate samples at a specific configuration level (100 ms to 5100 ms).

**show gsm-abis packets**

**show gsm-abis packets | include retransmit**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Examples</b>	The following <b>show gsm-abis packets</b> example shows the output generated by this command:
-----------------	--

```
Router# show gsm-abis packets
GSM-Abis(Serial0/2:0): packets:
  rxGSM_count ===== 164011
  txGSM_count ===== 164011
  rxBackhaul_packets ===== 163428
  txBackhaul_packets ===== 164011
  rxBackhaul_bytes ===== 7649833
  txBackhaul_bytes ===== 7638262
  rx_sampleCount ===== 40674728
  rx_suppressedCount ===== 36629047
  rx_retransmittedCount ===== 0
  rx_all_presentCount ===== 29
  tx_sampleCount ===== 4053144
  tx_presentCount ===== 66522
  tx_all_presentCount ===== 8
  backhaul_forced_inclusions == 1
  Last cleared 00:05:27
```

The following **show gsm-abis packets | include retransmit** example shows the output generated by this command:

```
Router# show gsm-abis packet | include retransmit
  rx-retransmittedCount ===== 71405
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear gsm-abis</b>	Clears the statistics displayed.

# show gsm-abis peering

To display the peering status, statistics, and history of GSM compression/decompression, use the **show gsm-abis peering** command in privileged EXEC mode.

**show gsm-abis peering [details]**

Syntax Description	details	(Optional) Provides detailed information about peering.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

## Examples

The following examples show the output generated by this command:

```
Router# show gsm-abis peering ser0/2:0
GSM-Abis(Serial0/2:0): Peering Information
GSM-Abis(Serial0/2:0): Local (10.10.10.1:5555) States:
GSM-Abis(Serial0/2:0): Connect State Is: CONNECTED
GSM-Abis(Serial0/2:0): Local Alarm Is: CLEAR (NO ALARM)
GSM-Abis(Serial0/2:0): Redundancy State: ACTIVE
GSM-Abis(Serial0/2:0): Local Peer Version: 1.0
GSM-Abis(Serial0/2:0): Remote (10.10.10.2:5555) States:
GSM-Abis(Serial0/2:0): Remote Alarm Is: CLEAR (NO ALARM)
GSM-Abis(Serial0/2:0): Remote Peer Version: 1.0

Router# show gsm-abis peering details ser0/2:0
GSM-Abis(Serial0/2:0): Peering Information (Version 1.0) History with current state at the
bottom GSM Peering History:

Connect State Is:                               System Time
-----
DISCONNECT *Apr 26 19:00:20.303
SND_CONNECT *Apr 26 15:48:30.568
ACK_CONNECT *Apr 26 15:48:31.572
**CONNECTED *Apr 26 15:50:57.113

Local Peer Is:      Conn Info      System Time
-----
CLEAR (NO ALARM)    DISCONNECT *Mar 1 19:00:20.303
SENDING AIS         DISCONNECT *Apr 24 15:48:31.980
**CLEAR (NO ALARM)  CONNECTED *Apr 26 15:51:04.113

Remote Peer Is:      Conn Info      Local Redundancy System Time
-----
UNAVAILABLE          DISCONNECT STANDBV *Mar 1 19:00:20.303
UNAVAILABLE          DISCONNECT ACTIVE *Mar 1 15:50:57.113
RX LOF RED) ALARM    CONNECTED ACTIVE *Apr 26 15:50:57.117
**CLEAR (NO ALARM)   CONNECTED ACTIVE *Apr 26 15:50:57.117

Current System Time:                               *Apr 26 16:00:33.133 est
```

```

Peer Pak Info:
No Backhaul Interface ===== 0 packets
Backhaul Encap Failures ===== 0 packets
Get CtrlPak Failures ===== 0 packets
RX Ctrl Paks ===== 7 packets
TX Ctrl Paks ===== 11 packets
  Out Of Sequence Paks ===== 1 packets
  Out Of Sequence Paks ===== 0 packets
Unsolicited Connect Paks ===== 1 (times)
  Unsolicited Connect Paks == 0 (times)
Remove Retransmit Errors ===== 8 (error)
Backhaul QOS classify drops = 0 packets

Peer Ctrl Type Info:
Unknown Ctrl Types ===== 0 (times)
Invalid Ctrl Lens ===== 0 (times)
Missed Keepalives ===== 0 (times)
Extra Keepalives ===== 0 (times)
Peer Restarts ===== 5 (times)
  Due to Cfg Change ===== 2(times)
  Due to Internal Err ===== 1(times)
  Due to Lost Keepalive ===== 0 (times)
  Due to Interface Down ===== 0 (times)
  Due to Critical Pak Lost == 0 (times)
  Due to Interface Cleanup == 0 (times)
  Due to Excess Seq No Err == 0 (times)

Peer Ctrl Variable Info:
peer_enable ===== 1 (on/off)
peer_ready ===== 1 (on/off)
connecting ===== 0 (on/off)
detectAlmErr ===== 1 (on/off)

Peer Queue/Memory Info:
Retransmission Contexts Used = 1 (in use)
Data Buffers Used ===== 0 (in use)
Seq Num: tx_fsn/tx_bsn ===== 4/4
Seq Num: rx_fsn/rx_bsn ===== 4/4
Adjacent serial number: 'FTX1021A44Q'

```

## Related Commands

Command	Description
<b>clear gsm-abis</b>	Clears the statistics displayed.

# show gsm-abis traffic

To display traffic rates, in bits per second, at intervals of 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour, for GSM data transmitted and received over the backhaul, use the **show gsm-abis traffic** command in privileged EXEC mode.

**show gsm-abis traffic**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows the output generated by this command:

```
Router# show gsm-abis traffic
```

```
GSM-Abis(Serial1/2:0): traffic (1sec/5sec/1min/5min/1hr) units(bps)
  compression traffic( 964000/ 966758/ 965928/ 965937/ 48831)
  decompression traffic( 132000/ 136774/ 134428/ 134430/ 6799)
```

Related Commands	Command	Description
	clear gsm-abis	Clears the statistics displayed.



# show interface switchport backup

Displays status information about the backup switchport.

**show interface switchport backup [detail]**

Syntax Description	detail	Provides additional information about the backup interface.
--------------------	--------	---

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows the output generated by this command:

```
Router# show interface switchport backup
```

```
Switch Backup Interface Pairs:
```

Active Interface	Backup Interface	State
-----		
GigabitEthernet0/0	GigabitEthernet0/5	Active Down/Backup Down

Related Commands	Command	Description
	<b>switchport backup interface</b>	Configures a backup interface pair.

# show ip rtp header-compression

To show Real-Time Transport Protocol (RTP) header compression statistics, use the **show ip rtp header-compression** privileged EXEC command.

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

Syntax Description	<i>type number</i>	(Optional) Interface type and number.
	<b>detail</b>	(Optional) Displays details of each connection.
	<b>Note</b>	This keyword is not supported on the Cisco MWR 2941-DC router. See “Usage Guidelines.”

Command Modes	Privileged EXEC
---------------	-----------------

Command History	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

**Usage Guidelines**

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

**Examples**

The following example shows output from the **show ip rtp header-compression** command:

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
Interface Multilink1 (compression off, IETF, RTP)
  Rcvd: 0 total, 0 compressed, 0 errors
        0 dropped, 0 buffer copies, 0 buffer failures
  Sent: 430 total 429 compressed
        15122 bytes saved, 0 bytes sent
        0 efficiency improvement factor
  Connect: 16 rx slots, 16 tx slots, 0 long searches, 1 misses
        99% hit ratio, five minute miss rate 0 misses/sec, 0 max.
```

Table A-3 describes the significant fields shown in the display.

**Table A-3** show ip rtp header-compression Field Descriptions

Field	Description
Interface	Type and number of the interface.
Rcvd: total	Number of packets received on the interface.
compressed	Number of packets with compressed headers.

**Table A-3** *show ip rtp header-compression Field Descriptions (continued)*

Field	Description
errors	Number of errors.
dropped	Number of dropped packets.
buffer copies	Not applicable to the Cisco MWR 2941-DC router.
buffer failures	Not applicable to the Cisco MWR 2941-DC router.
Sent: total	Total number of packets sent.
compressed	Number of packets sent with compressed headers.
bytes saved	Total savings in bytes as a result of compression.
bytes sent	Not applicable to the Cisco MWR 2941-DC router.
efficiency improvement factor	Efficiency achieved through compression.
Connect: rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
long searches	Not applicable to the Cisco MWR 2941-DC router.
misses	Number of new states that were created.
hit ratio	Number of times that existing states were revised.
five minute miss rate	Average miss rate.
max.	Maximum miss rate.
negative cache	Not applicable to the Cisco MWR 2941-DC router.

**Related Commands**

Command	Description
<b>ip rtp compression-connections</b>	Specifies the total number of RTP header compression connections that can exist on an interface.
<b>ip rtp header-compression</b>	Enables RTP header compression.

# show mpls l2transport vc

To display information about Any Transport over MPLS (AToM) virtual circuits (VCs) that have been enabled to route Layer 2 packets on a router, use the **show mpls l2transport vc** command in privileged EXEC mode.

**show mpls l2transport vc** [**vcid** *vc-id*] | [**vcid** *vc-id-min vc-id-max*] [**interface** *name* [*local-circuit-id*]] [**destination** *ip-address* | *name*] [**detail**]

Syntax Description	
<b>vcid</b>	(Optional) Allows you to enter a specific VC ID to display.
<i>vc-id</i>	(Optional) The VC ID number.
<i>vc-id-min</i> <i>vc-id-max</i>	(Optional) Allows you to enter a range of VCs to display. The range is from 1 to 4294967295. (This argument is primarily used for legacy implementations.)
<b>interface</b>	(Optional) The interface or subinterface of the router that has been enabled to transport Layer 2 packets. This keyword lets you display information about the VCs that have been assigned VC IDs on that interface or subinterface.
<i>name</i>	(Optional) The name of the interface or subinterface.
<i>local-circuit-id</i>	(Optional) The number assigned to the local circuit. This argument value is supported only by the following transport types: <ul style="list-style-type: none"> <li>For ATM adaptation layer 5 (AAL5) and cell relay, enter the virtual path identifier (VPI)/virtual channel identifier (VCI) of the PVC.</li> <li>For Ethernet VLANs, enter the VLAN number.</li> </ul>
<b>destination</b>	(Optional) Information about the VCs that have been assigned VC IDs for the remote router you specify.
<i>ip-address</i>	(Optional) The IP address of the remote router.
<i>name</i>	(Optional) The name assigned to the remote router.
<b>detail</b>	(Optional) Detailed information about the VCs that have been assigned VC IDs.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Usage Guidelines** If you do not specify any keywords or arguments, the command displays a summary of all the VCs.

**Examples** The output of the commands varies, depending on the type of Layer 2 packets being transported over the AToM VCs.

The following example shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router:

```
Router# show mpls l2transport vc
```

Local intf	Local circuit	Dest address	VC ID	Status
AT4/0	ATM AAL5 0/100	10.0.0.1	100	UP
AT4/0	ATM AAL5 0/200	10.0.0.1	200	UP
AT4/0.300	ATM AAL5 0/300	10.0.0.1	300	UP

Table A-4 describes the significant fields shown in the display.

**Table A-4** *show mpls l2transport vc Field Descriptions*

Field	Description
Local intf	The interface on the local router that has been enabled to transport Layer 2 packets.
Local circuit	The type and number (if applicable) of the local circuit. The output shown in this column varies, depending on the transport type: <ul style="list-style-type: none"> <li>For ATM cell relay and AAL5, the output shows the VPI/VCI of the PVC.</li> <li>For Ethernet VLANs, the output shows the VLAN number.</li> </ul>
Dest address	The IP address of the remote router's interface that is the other end of the VC.
VC ID	The VC identifier assigned to one of the interfaces on the router.
Status	The status of the VC. The status can be one of the following conditions: <ul style="list-style-type: none"> <li>UP—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed. <ul style="list-style-type: none"> <li>The disposition interface is programmed if the VC has been configured and the client interface is up.</li> <li>The imposition interface is programmed if the disposition interface is programmed and you have a remote VC label and an Interior Gateway Protocol (IGP) label. The IGP label can be implicit null in a back-to-back configuration. An IGP label means there is a Label Switched Path (LSP) to the peer.</li> </ul> </li> <li>DOWN—The VC is not ready to carry traffic between the two VC endpoints. Use the <b>detail</b> keyword to determine the reason that the VC is down.</li> <li>ADMIN DOWN—The VC has been disabled by a user.</li> <li>RECOVERING—The VC is recovering from a stateful switchover.</li> </ul>

The following example shows information about the NSF/SSO and graceful restart capability. The SSO portion indicates when checkpointing data has either been sent (on active) or received (on standby). When SSO data has not been successfully sent or has been released, the SSO information is not shown.

Router# **show mpls l2transport vc detail**

```

Local interface: Fa0/1.1 down, line protocol down, Eth VLAN 2 up
  Destination address: 10.55.55.2, VC ID: 1002, VC status: down
    Output interface: Fa0/0, imposed label stack {16}
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop point2point
  Create time: 02:03:29, last status change time: 02:03:26
  Signaling protocol: LDP, peer 10.55.55.2:0 down
    MPLS VC labels: local 16, remote unassigned
    Group ID: local 0, remote unknown

```

```

MTU: local 1500, remote unknown
Remote interface description:
Sequencing: receive disabled, send disabled
SSO Descriptor: 10.55.55.2/1002, local label: 16
SSM segment/switch IDs: 12290/8193, PWID: 8193
VC statistics:
  packet totals: receive 0, send 0
  byte totals:   receive 0, send 0
  packet drops:  receive 0, send 0

```

Table A-5 describes the significant fields shown in the display.

**Table A-5** *show mpls l2transport vc Field Descriptions*

Field	Description
Local interface	Interface on the local router that has been enabled to send and receive Layer 2 packets. The interface varies, depending on the transport type. The output also shows the status of the interface.
line protocol	Status of the line protocol on the edge-facing interface.
Destination address	IP address of the remote router specified for this VC. Specify the destination IP address as part of the <b>mpls l2transport route</b> command.
VC ID	VC identifier assigned to the interface on the router.
VC status	<p>Status of the VC, which is one of the following conditions:</p> <p>UP—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed.</p> <ul style="list-style-type: none"> <li>The disposition interface is programmed if the VC has been configured and the client interface is up.</li> <li>The imposition interface is programmed if the disposition interface is programmed and a remote VC label and an IGP label exist. The IGP label can be an implicit null in a back-to-back configuration. (An IGP label means there is an LSP to the peer.)</li> </ul> <p>DOWN—The VC is not ready to carry traffic between the two VC endpoints.</p> <p>ADMIN DOWN—The VC has been disabled by a user.</p>
Output interface	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
imposed label stack	Summary of the MPLS label stack used to direct the VC to the PE router.
Preferred path	Path that was assigned to the VC and the status of that path. The path can be an MPLS traffic engineering tunnel or an IP address or hostname of a PE router.
Default path	<p>Status of the default path, which can be disabled or active.</p> <p>By default, if the preferred path fails, the router uses the default path. However, you can disable the router from using the default path when the preferred path fails by specifying the <b>disable-fallback</b> keyword with the <b>preferred-path</b> command.</p>
Create time	Time when the VC was provisioned.
last status change time	Last time the VC state changed.

**Table A-5** *show mpls l2transport vc Field Descriptions (continued)*

Field	Description
Signaling protocol	Type of protocol used to send the MPLS labels. The output also shows the status of the peer router.
MPLS VC labels	Local VC label is a disposition label, which determines the egress interface of an arriving packet from the MPLS backbone. The remote VC label is a disposition VC label of the remote peer router.
Group ID	Local group ID is used to group VCs locally. The remote group ID is used by the peer to group several VCs.
MTU	Maximum transmission unit specified for the local and remote interfaces.
Remote interface description	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
Tunnel label	<p>An IGP label used to route the packet over the MPLS backbone to the destination router with the egress interface. The first part of the output displays the type of label. The second part of the output displays the route information.</p> <p>The tunnel label information can display any of the following states:</p> <ul style="list-style-type: none"> <li>• imp-null—The provider (P) router is absent and the tunnel label is not to be used. Alternatively, imp-null can signify traffic engineering tunnels between the PE routers.</li> <li>• unassigned—The label has not been assigned.</li> <li>• no route—The label is not in the routing table.</li> <li>• no adjacency—The adjacency for the next hop is missing.</li> <li>• not ready, no route—An IP route for the peer does not exist in the routing table.</li> <li>• not ready, not a host table—The route in the routing table for the remote peer router is not a host route.</li> <li>• not ready, Cisco Express Forwarding disabled—Cisco Express Forwarding is disabled.</li> <li>• not ready, label forwarding information base (LFIB) disabled—The MPLS switching subsystem is disabled.</li> <li>• not ready, LFIB entry present—The tunnel label exists in the LFIB, but the VC is down.</li> </ul>
SSO Descriptor	Identifies the VC for which the information was checkpointed.
local label	The value of the local label that was checkpointed (that is, sent on the active Route Processor [RP], and received on the standby RP).
SSM segment/switch IDs	The IDs used to refer to the control plane and data plane contexts for this VC. This data is not for customer use but for Cisco personnel for troubleshooting purposes. When the source specific multicast (SSM) IDs are followed by the word “used,” the checkpointed data has been successfully sent and not released.
PWID	The PW ID used in the data plane to correlate the switching context for the segment mentioned with the MPLS switching context. This data is not for customer use but for Cisco personnel for troubleshooting purposes.

**Table A-5** *show mpls l2transport vc Field Descriptions (continued)*

Field	Description
packet totals	Number of packets sent and received. Received packets are those AToM packets received from the MPLS core. Sent packets are those AToM packets sent to the MPLS core. This number does not include dropped packets.
byte totals	Number of bytes sent and received from the core-facing interface, including the payload, control word if present, and AToM VC label.
packet drops	Number of dropped packets.

**Related Commands**

Command	Description
<b>show mpls l2transport summary</b>	Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a router.



# show network-clocks

To display information about the network clocks configured on the router, use the **show network-clocks** command. The command shows the priority and state of all configured clocks and the currently selected clock.

**show network-clocks**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	Privileged EXEC
----------------------	-----------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Examples</b>	The following example shows how to use the set network-clock-select force-reselect command: Router# <b>show network-clocks</b>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>set network-clock-select force-reselect</b>	This command causes the router to reselect a network clock.

# show platform hardware

To display the status of hardware devices on the Cisco MWR 2941-DC, use the **show platform hardware** command. The command displays information about hardware devices on the Cisco MWR 2941-DC for troubleshooting and debugging purposes.

**show platform hardware {adrian | bits | cpld | cpu | ethernet | fio | hwic | rtm | stratum | ufe winpath} [detail] [stats]**

Syntax Description	
<b>adrian</b>	Displays information about the adrian hardware.
<b>bits</b>	Displays information about the BITS hardware.
<b>cpld</b>	Displays information about the CPLD hardware.
<b>cpu</b>	Displays information about the CPU.
<b>ethernet</b>	Displays information about the ethernet interfaces on the Cisco MWR 2941-DC.
<b>fio</b>	Displays information about the FIO fpga hardware.
<b>hwic</b>	Displays information about the HWICs installed on the Cisco MWR 2941-DC.
<b>rtm</b>	Displays information about the RTM Module (ASM-M2900-TOP daughter card).
<b>stratum</b>	Displays information about the stratum hardware.
<b>ufe</b>	Displays information about the UFE hardware.
<b>winpath</b>	Displays information about the Winpath hardware.
<b>detail</b>	Display additional detail about Cisco MWR 2941-DC hardware.
<b>stats</b>	Displays RTM statistics.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

Related Commands	Command	Description
	<b>show controller</b>	Displays the status of system controllers.

# show ptp clock

Displays information about the PTP clock.

**show ptp clock**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	Release	Modification
	12.4(12)MR2	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>show ptp clock</b> command to display information about the PTP clock.
-------------------------	---

<b>Examples</b>	<pre>Router# show ptp clock PTP CLOCK INFO PTP Device Type: Ordinary clock Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E Clock Domain: 2 Number of PTP ports: 1 Priority1: 128 Priority2: 128 Clock Quality:   Class: 13   Accuracy: Within 1s   Offset (log variance): 52592 Offset From Master: 0 Mean Path Delay: 0 Steps Removed: 0 Local clock time: 19:58:40 UTC Oct 30 2000</pre>
-----------------	---

<b>Related Commands</b>	Command	Description
	<a href="#">show ptp foreign-master-record</a>	Displays the PTP foreign master records.
	<a href="#">show ptp parent</a>	Displays the PTP parent properties.
	<a href="#">show ptp port</a>	Displays the PTP port properties.
	<a href="#">show ptp time-property</a>	Displays the time properties of the PTP clock.

# show ptp foreign-master-record

To display the PTP foreign master record set, use the **show ptp foreign-master-record** command in user EXEC mode.

**show ptp foreign-master-record**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.4(12)MR2	This command was introduced.

**Usage Guidelines** Use the **show ptp foreign-master-record** command to display the PTP foreign master records.

**Examples** The following example shows output from the **show ptp foreign-master-record** command:

```
Router# show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface Vlan2
Number of foreign records 1, max foreign records 5
Best foreign record 0
RECORD #0
Foreign master port identity: clock id: 0x0:1E:4A:FF:FF:96:D2:A9
Foreign master port identity: port num: 1
Number of Announce messages: 8
Number of Current Announce messages: 6
Time stamps: 1233935406, 664274927
```

Related Commands	Command	Description
	<a href="#">show ptp clock</a>	Displays information about the PTP clock.
	<a href="#">show ptp parent</a>	Displays the PTP parent properties.
	<a href="#">show ptp port</a>	Displays the PTP port properties.
	<a href="#">show ptp time-property</a>	Displays the time properties of the PTP clock.

# show ptp parent

To display the properties of the PTP parent, use the **show ptp parent** command in user EXEC mode.

## show ptp parent

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	Release	Modification
	12.4(12)MR2	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>show ptp parent</b> command to display the properties of the PTP parent.
-------------------------	---

<b>Examples</b>	The following example shows output from the <b>show ptp parent</b> command:
-----------------	---

```
Router# show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
    Parent Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E
    Parent Port Number: 0
    Observed Parent Offset (log variance): N/A
    Observed Parent Clock Phase Change Rate: 0

  Grandmaster Clock:
    Grandmaster Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E
    Grandmaster Clock Quality:
      Class: 248
      Accuracy: Greater than 10s
      Offset (log variance): 52592
      Priority1: 128
      Priority2: 128
```

<b>Related Commands</b>	Command	Description
	<a href="#">show ptp clock</a>	Displays information about the PTP clock.
	<a href="#">show ptp foreign-master-record</a>	Displays the PTP foreign master records.
	<a href="#">show ptp port</a>	Displays the PTP port properties.
	<a href="#">show ptp time-property</a>	Displays the time properties of the PTP clock.

# show ptp port

To display the PTP port properties, use the **show ptp port** command in user EXEC mode.

**show ptp port**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC

Command History	Release	Modification
	12.4(12)MR2	This command was introduced.

**Usage Guidelines** Use the **show ptp port** command to display the PTP port properties.

**Examples** The following example shows output from the **show ptp port** command:

```
Router# show ptp port
PTP PORT DATASET: Vlan1
  Port identity: clock identity: 0x0:1E:4A:FF:FF:96:A9:9E
  Port identity: port number: 1
  PTP version: 2
  Delay request interval(log mean): 0
  Announce receipt time out: 0
  Peer mean path delay: 0
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 6000
```

Related Commands	Command	Description
	<a href="#">show ptp clock</a>	Displays information about the PTP clock.
	<a href="#">show ptp foreign-master-record</a>	Displays the PTP foreign master records.
	<a href="#">show ptp parent</a>	Displays the PTP parent properties.
	<a href="#">show ptp time-property</a>	Displays the time properties of the PTP clock.

# show ptp time-property

To display the PTP clock time properties, use the **show ptp time-property** command in user EXEC mode.

## show ptp time-property

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	User EXEC
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(12)MR2	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>show ptp time-property</b> command to display PTP clock time properties.
-------------------------	---

<b>Examples</b>	The following example shows output from the <b>ptp time-property</b> command:
-----------------	---

```
Router# show ptp time-property
PTP CLOCK TIME PROPERTY
Current UTC offset valid: 1
Current UTC offset: 33
Leap 59: 0
Leap 61: 0
Time Traceable: 0
Frequency Traceable: 1
PTP Timescale: 1
Time Source: Hand Set
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show ptp clock</a>	Displays information about the PTP clock.
	<a href="#">show ptp foreign-master-record</a>	Displays the PTP foreign master records.
	<a href="#">show ptp parent</a>	Displays the PTP parent properties.
	<a href="#">show ptp port</a>	Displays the PTP port properties.

# show xconnect all

To display information about xconnect attachment circuits and pseudowires (PWs), use the **show xconnect all** command in privileged EXEC mode.

```
show xconnect {all | interface interface | peer ip-address {all | vcid vcid}} [detail]
```

Syntax Description

all	Displays information about all xconnect attachment circuits and PWs.
interface interface	Displays information about xconnect attachment circuits and PWs on the specified interface. Valid values for the argument are as follows: <ul style="list-style-type: none"><li>atm number—Displays xconnect information for a specific ATM interface or subinterface.</li><li>atm number vp vpi-value—Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). This command does not display information about virtual connect (VC) xconnects using the specified VPI.</li><li>atm number vp vpi-value/vci-value—Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination.</li><li>ethernet number—Displays port-mode xconnect information for a specific Ethernet interface or subinterface.</li><li>gigabitethernet number—Displays port-mode xconnect information for a specific Fast Ethernet interface or subinterface.</li><li>serial number—Displays xconnect information for a specific serial interface.</li><li>serial number dlci-number—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).</li></ul>
peer ip-address {all   vcid vcid}	Displays information about xconnect attachment circuits and PWs associated with the specified peer IP address. <ul style="list-style-type: none"><li>all—Displays all xconnect information associated with the specified peer IP address.</li><li>vcid vcid—Displays xconnect information associated with the specified peer IP address and the specified VC ID.</li></ul>
detail	(Optional) Displays detailed information about the specified xconnect attachment circuits and PWs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

The **show xconnect all** command can be used to display, sort, and filter basic information about all xconnect attachment circuits and PWs.



You can use the **show xconnect all** command output to help determine the appropriate steps to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the "Related Commands" table.

## Examples

The following example shows **show xconnect all** command output in the brief (default) display format. The output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router.

```
Router# show xconnect all
```

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State

UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware

XC	ST	Segment 1	S1	Segment 2	S2
----	----	-----------	----	-----------	----

ST	Segment 1		S1	Segment 2	S2
UP	ac	Et0/0(Ethernet)	UP	mpls 10.55.55.2:1000	UP
UP	ac	Et1/0.1:200(Eth VLAN)	UP	mpls 10.55.55.2:5200	UP
IA pri	ac	Et1/0.2:100(Eth VLAN)	UP	ac Et2/0.2:100(Eth VLAN)	UP
UP sec	ac	Et1/0.2:100(Eth VLAN)	UP	mpls 10.55.55.3:1101	UP

Table A-6 describes the significant fields shown in the display.

**Table A-6**      *show xconnect all Field Descriptions*

Field	Description
XC ST	<ul style="list-style-type: none"> <li>State of the xconnect attachment circuit or PW. Valid states are:</li> <li>UP—The xconnect attachment circuit or PW is up. Both segment 1 and segment 2 must be up for the xconnect to be up.</li> <li>DN—The xconnect attachment circuit or PW is down. Either segment 1, segment 2, or both segments are down.</li> <li>IA—The xconnect attachment circuit or PW is inactive. This state is valid only when PW redundancy is configured.</li> <li>NH—One or both segments of this xconnect no longer has the required hardware resources available to the system.</li> </ul>
Segment 1 or Segment 2	<p>Information about the type of xconnect, the interface type, and the IP address the segment is using. Types of xconnects are:</p> <ul style="list-style-type: none"> <li>ac—Attachment circuit.</li> <li>pri ac—Primary attachment circuit.</li> <li>sec ac—Secondary attachment circuit.</li> <li>mpls—Multiprotocol Label Switching.</li> <li>l2tp—Layer 2 Tunnel Protocol.</li> </ul>
S1 or S2	<p>State of the segment. Valid states are:</p> <ul style="list-style-type: none"> <li>UP—The segment is up.</li> <li>DN—The segment is down.</li> <li>AD—The segment is administratively down.</li> </ul>

The following example shows **show xconnect all** command output in the detailed display format:

# show xconnect all

Router# **show xconnect all detail**

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State

UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No HardwareXC

ST	Segment 1	S1	Segment 2	S2
UP	ac Et0/0 (Ethernet) Interworking: ip	UP mpls	10.55.55.2:1000 Local VC label 16 Remote VC label 16 pw-class: mpls-ip	UP
UP	ac Et1/0.1:200 (Eth VLAN) Interworking: ip	UP mpls	10.55.55.2:5200 Local VC label 17 Remote VC label 20 pw-class: mpls-ip	UP
IA pri	ac Et1/0.2:100 (Eth VLAN) Interworking: none	UP ac	Et2/0.2:100 (Eth VLAN) Interworking: none	UP
UP sec	ac Et1/0.2:100 (Eth VLAN) Interworking: none	UP mpls	10.55.55.3:1101 Local VC label 23 Remote VC label 17 pw-class: mpls	UP

The additional fields displayed in the detailed output are self-explanatory.

## Related Commands

Command	Description
<b>show atm pvc</b>	Displays all ATM PVCs and traffic information.
<b>show atm vc</b>	Displays all ATM PVCs and SVCs and traffic information.
<b>show atm vp</b>	Displays the statistics for all VPs on an interface or for a specific VP.
<b>show connect</b>	Displays configuration information about drop-and-insert connections that have been configured on a router.
<b>show frame-relay pvc</b>	Displays statistics about PVCs for Frame Relay interfaces.
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.
<b>show mpls l2transport binding</b>	Displays VC label binding information.
<b>show mpls l2transport vc</b>	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

# snmp-server enable traps ipran

To enable all ipran notifications through Simple Network Management Protocol (SNMP) notifications (traps) available on your system, use the **snmp-server enable traps ipran** command in global configuration mode. To disable ipran notifications, use the **no** form of this command.

**snmp-server enable traps ipran**

**no snmp-server enable traps ipran**

**Related Commands** This command has no arguments or keywords.

**Defaults** This command is disabled by default. No notifications are sent.

**Command Modes** Global configuration

Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.

**Examples** The following example shows the output generated by this command:

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

Related Commands	Command	Description
	<b>snmp-server enable traps ipran alarm-gsm</b>	Provides information alarms associated with GSM-Abis interfaces.
	<b>snmp-server enable traps ipran util</b>	Provides information on backhaul utilization.

# snmp-server enable traps ipran alarm-gsm

To provide information alarms associated with GSM-Abis interfaces through Simple Network Management Protocol (SNMP) notifications (traps) available on your system, use the **snmp-server enable traps ipran alarm-gsm** command in global configuration mode. To disable ipran alarm-gsm notifications, use the **no** form of this command.

**snmp-server enable traps ipran alarm-gsm**

**no snmp-server enable traps ipran alarm-gsm**

This statement controls the generation of the cisco IpRanBackHaulGsmAlarm notification from the CISCO-IP-RAN-BACKHAUL-MIB.

Syntax Description	This command has no arguments or keywords.	
Defaults	This command is disabled by default. No notifications are sent.	
Command Modes	Global configuration	
Command History	Release	Modification
	12.4(19)MR2	This command was incorporated.
Examples	<p>The following example shows the output generated by this command:</p> <pre>Router(config)# snmp-server enable traps ipran alarm-gsm</pre>	
Related Commands	Command	Description
	snmp-server enable traps ipran util	Provides information on backhaul utilization.
	snmp-server enable traps ipran	Enables all notifications.

# snmp-server enable traps ipran util

To provide information alarms associated with backhaul utilization through Simple Network Management Protocol (SNMP) notifications (traps) available on your system, use the **snmp-server enable traps ipran util** command in global configuration mode. To disable ipran utilization notifications, use the **no** form of this command.

**snmp-server enable traps ipran util**

**no snmp-server enable traps ipran util**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	This command is disabled by default. No notifications are sent.
-----------------	---

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(19)MR2	This command was incorporated.

<b>Examples</b>	The following example shows the output generated by this command:
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>snmp-server enable traps ipran alarm-gsm</b>	Provides information alarms associated with GSM-Abis interfaces.
	<b>snmp-server enable traps ipran</b>	Enables all notifications.
	<b>ipran-mib backhaul-notify-interval</b>	Specifies the interval used to calculate the utilization.
	<b>ipran-mib threshold-acceptable</b>	Specifies the acceptable level of traffic.
	<b>ipran-mib threshold-overloaded</b>	Specifies the amount of traffic that indicates the backhaul is overloaded.
	<b>ipran-mib threshold-warning</b>	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.

# switchport backup interface

Use the **switchport backup interface** interface configuration command on a Layer 2 interface to configure Flex Links, a pair of interfaces that provide backup to each other. Use the **no** form of this command to remove the Flex Links configuration.

**switchport backup interface** *{interface-id}* **preemption** **{delay** *delay-time* **| mode** **{bandwidth | forced | off}}**

**no switchport backup interface** *{interface-id}* **preemption** **{delay** *delay-time* **| mode** **{bandwidth | forced | off}}**

## Syntax Description

<i>interface-id</i>	The Layer 2 interface that acts as a backup link to the interface being configured. The interface can be a physical interface or port channel. The port-channel range is 1–486.
<b>preemption</b>	Configures a preemption scheme for a backup interface pair.
<b>delay</b>	(Optional) Specifies a preemption delay.
<i>delay-time</i>	(Optional) Specifies the length of the preemption delay; valid values are 1–300 seconds.
<b>mode</b>	Specifies the preemption mode as bandwidth, forced, or off.
<b>bandwidth</b>	(Optional) Specifies that the interface with the higher available bandwidth always preempts the backup.
<b>forced</b>	(Optional) Specifies that the interface always preempts the backup.
<b>off</b>	(Optional) Specifies that no preemption occurs from backup to active.

## Defaults

There is no default setting.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Examples

The following example shows the output generated by this command:

```
Router(config)# interface gigabitethernet0/3
Router(config-if)# switchport backup interface gigabitethernet0/4
```

## Related Commands

Command	Description
<b>show interface switchport backup</b>	Displays status information about the backup switchport.

# xconnect

To bind an attachment circuit to a pseudowire, use the **xconnect** command in one of the supported configuration modes. To restore the default values, use the **no** form of this command.

**xconnect** *peer-ip-address* | *vcid* | *pseudowire-parameters* [**ignore-vpi-vci**]

**no xconnect**

## Syntax Description

<i>peer-ip-address</i>	IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.
<i>vcid</i>	The 32-bit identifier of the virtual circuit (VC) between the PE routers.
<i>pseudowire-parameters</i>	Encapsulation and pseudowire-class parameters to be used for the attachment circuit. At least one of the following PW parameters must be configured: <ul style="list-style-type: none"> <li><b>encapsulation</b> {<b>l2tpv3</b>   <b>mpls</b>}— Specifies the tunneling method to encapsulate the data in the PW: <ul style="list-style-type: none"> <li><b>l2tpv3</b>—Specifies L2TPv3 as the tunneling method.</li> <li><b>mpls</b>—Specifies MPLS as the tunneling method.</li> </ul> </li> </ul> <p><b>Note</b> L2TP is not currently supported on the Cisco MWR 2941-DC.</p> <ul style="list-style-type: none"> <li><b>pw-class</b> <i>pw-class-name</i>—Specifies the pseudowire-class configuration from which the data encapsulation type is taken. This option is mandatory if you select an encapsulation method.</li> </ul>
<b>transmit</b>	Sequences data packets received from the attachment circuit.
<b>receive</b>	Sequences data packets sent into the attachment circuit.
<b>both</b>	Sequences data packets that are both sent and received from the attachment circuit.
<b>one-to-one</b>	Applies only when the <b>xconnect</b> command is configured under the AAL0 encapsulation PVC. The keyword specifies the PW type as a one-to-one VCC cell relay.
<b>ignore-vpi-vci</b>	This parameter sets the Cisco MWR 2941-DC to ignore the VPI/VCI value in the PW packet and rewrite the egress ATM cell header with VPI/VCI value of the locally configured (attachment side) PVC. <p><b>Note</b> You can only use this parameter for a 1-to-1 pseudowire, for which you apply the xconnect command to a PVC.</p>

## Defaults

The attachment circuit is not bound to the PW.

## Command Modes

CEM circuit configuration  
Interface configuration  
Subinterface configuration  
l2transport configuration (for ATM)

Connect configuration  
Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each xconnect configuration must have a unique combination of peer IP address and VCID configuration.



Note

If the remote router is a Cisco 12000 series Internet router, the *peer-ip-address* argument must specify a loopback address on the router.

The same *vcid* value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE routers. The *vcid* argument creates the binding between a PW and an attachment circuit.

The **pw-class** *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire-class. In this way, the pseudowire-class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **xconnect** command.



Note

If you specify the encapsulation keywords, you must specify the **pw-class** keyword.

ignore-vpi-vci Keyword

Using the **xconnect** command with the **ignore-vpi-vci** keyword provides benefits over using the **pw-pvc** command for PVC mapping.

Originally, PVC mapping was done through the **pw-pvc pw-vpi/pw-vci** command. When the MWR received the MPLS PW packet, it decoded the PW payload and looked up the PW VPI/VCi value to see if it matched any local configured PVC values. If a match was made, the PW-VPI/PW-VCi was translated to the AC-side VPI/VCi and the cell was sent to the local PVC. Without a match, the MWR dropped the received PW packet. When the MWR generated the PW packet, it used configured **pw-vpi/pw-vci** values. In this case, the PVC mapping was done completely on the MWR and was transparent to the remote end.

The process changes when the **ignore-vpi-vci** keyword is configured. For N:1 with N=1 special case, when the PW packet is received from the MWR, the receiving router ignores the VPI/VCi value contained in the PW payload. It does a blind rewrite to use the AC-side VPI/VCi and sends the cell to the AC side PVC.

The **xconnect** command with the **ignore-vpi-vci** keyword results in the PVC mapping being done in a cooperative way if the MWR works the same way as the receiving router. Without this command, the MWR checks the VPI/VCi value inside the PW packet for matches against the local configured PVC or PVC-mapping. With the **ignore-vpi-vci** keyword configured, the MWR ignores the VPI/VCi header inside the received PW packet and does a blind rewrite with the local configured AC-side PVC's VPI/VCi value.



Note

This process applies only to N:1 VCC PW with N=1 special case.



## Examples

The following example configures **xconnect** service for an ATM interface by binding the ATM circuit to the PW named 123 with a remote peer 10.0.3.201. The configuration settings in the pseudowire class named ATM-xconnect are used.

```
Router# config tby
Router(config)# interface ATM 0/0
Router(config-if)# xconnect 10.0.3.201 123 pw-class ATM-xconnect
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

The following example illustrates PVC mapping using the **ignore-vpi-vci** keyword with the **xconnect** command. The example shows both the MWR and remote end (7600) routers.

MWR:

```
Router# config t
Router(config)# interface ATM 0/0
Router(config-if)# pvc 0/10 12transport
Router(config-if-atm-12trans-pvc)# encapsulation aa10
Router(config-if-atm-12trans-pvc)# xconnect 10.10.10.10 100 encapsulation mpls ignore-vpi-vci
Router(config-if-atm-12trans-pvc-xconn)# exit
Router(config-if-atm-12trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

7600:

```
Router# config t
Router(config)# interface ATM 0/0
Router(config-if)# pvc 2/20 12transport
Router(config-if-atm-12trans-pvc)# encapsulation aa10
Router(config-if-atm-12trans-pvc)# xconnect 20.20.20.20 100 encapsulation mpls
Router(config-if-atm-12trans-pvc-xconn)# exit
Router(config-if-atm-12trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

## Related Commands

Command	Description
<b>pseudowire-class</b>	Configures a template of PW configuration settings used by the attachment circuits transported over a PW.
<b>show xconnect</b>	Displays information about xconnect attachment circuits and PWs.

# xconnect logging redundancy

To enable system message log (syslog) reporting of the status of the xconnect redundancy group, use the **xconnect logging redundancy** command in global configuration mode. To disable syslog reporting of the status of the xconnect redundancy group, use the **no** form of this command.

**xconnect logging redundancy**

**no xconnect logging redundancy**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Syslog reporting of the status of the xconnect redundancy group is disabled.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

## Usage Guidelines

Use this command to enable syslog reporting of the status of the xconnect redundancy group.

## Examples

The following example enables syslog reporting of the status of the xconnect redundancy group and shows the messages that are generated during switchover events:

```
Router# config t
Router(config)# xconnect logging redundancy
Router(config)# exit
```

### Activating the Primary Member

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

### Activating the Backup Member:

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

## Related Commands

Command	Description
<b>xconnect</b>	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an Layer 2 PW for xconnect service and enters xconnect configuration mode.



# APPENDIX **B**

## Configuration Examples

---

The Cisco MWR 2941-DC supports a variety of topology designs based on various GSM configurations, including the following common topologies:

- A *backhaul* interface is used to transfer optimized GSM traffic between RAN-O devices. The traditional backhaul interface is comprised of one or more T1/E1 controllers logically combined to form a *multilink* connect (except HSDPA, which uses the backhaul interface for T1/E1 line clocking).
- A *shorthaul* interface is used to transfer GSM traffic from the BTS/Node-B to the Cisco MWR 2941-DC router and from the Cisco MWR 2941-DC router to the BSC/RNC. The traditional shorthaul connections on the RAN-O devices are connected through the Cisco T1/E1 interface card.
- Topology naming conventions such as 3x2 and 4x3 are used to describe the type of deployment. The first number signifies the number of GSM shorthaul interface connections and the second number signifies the number of multilink backhaul interface connections.

## Examples

This appendix includes examples of the following real-world RAN-O configurations:



**Note**

---

The Cisco MWR 2941-DC does not currently support L2TP as shown in some of the following examples.

---

- [Asymmetric PWE3 Configuration, page B-2](#)
- [PWE3 Redundancy Configuration, page B-15](#)
- [TDM over MPLS Configuration, page B-21](#)
- [ATM over MPLS Configuration, page B-25](#)
- [GSM-Only Configuration, page B-32](#)
- [GSM-Only Configuration Using Satellite, page B-36](#)
- [GSM Congestion Management, page B-39](#)



**Note**

---

The network addresses in these examples are generic addresses, so you must replace them with actual addresses for your network.

---

## B-2

OL-18665-01

The diagram illustrates the network topology for the MWR\_1 and MWR\_2 nodes. It shows a connection between BTS/Node B and BSC/RNC via two intermediate nodes, MWR\_1 and MWR\_2. The connections are labeled ATM and TDM. Arrows indicate FE0/0 (Uplink) and FE0/1 (Downlink) directions.

```
version 12.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname MWR1
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
card type e1 1 0
card type e1 1 1
logging buffered 2147483
!
no aaa new-model
memory-size iomem 25
!
network-clock-select 1 E1 1/3
!
ipran-alt-interrupt tracing
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
!
no ip domain lookup
vlan ifdescr detail
multilink bundle-name authenticated
mpls label protocol ldp
vpdn enable
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
archive
  log config
!
!
controller E1 0/0
  clock source internal
  cem-group 1 unframed
!
controller E1 0/1
  clock source internal
  cem-group 20 unframed
!
controller E1 0/2
  clock source internal
  cem-group 12 unframed
  description connected to E1 4/0 of BERT
!
controller E1 0/3
  clock source internal
  cem-group 30 unframed
!
controller E1 0/4
  clock source internal
  cem-group 8 unframed
!
controller E1 0/5
  clock source internal
  cem-group 25 unframed
!
controller E1 1/0
  mode aim 1
  clock source internal
!
controller E1 1/1
  mode aim 1
  clock source internal
!
controller E1 1/2
  mode aim 1
  clock source internal
!
controller E1 1/3
!
!
pseudowire-class mpls
  encapsulation mpls
  preferred-path peer 50.0.0.2
!
pseudowire-class l2tp
  encapsulation mpls
  ip protocol udp
  ip local interface Loopback50
!
!
class cem cemclass
```

```
payload-size 32
!
class cem cemclass1
  de jitter-buffer 400
!
!
!
!
!
!
interface Loopback50
  ip address 50.0.0.1 255.255.255.255
!
interface CEM0/0
  no ip address
  cem 1
  xconnect 50.0.0.2 1 encapsulation mpls
!
!
interface GigabitEthernet0/0
  ip address 20.0.0.1 255.0.0.0
  load-interval 30
  duplex auto
  speed auto
  mpls label protocol ldp
  mpls ip
!
interface CEM0/1
  no ip address
  cem 20
  xconnect 50.0.0.2 2 encapsulation mpls
!
interface GigabitEthernet0/1
  ip address 60.0.0.1 255.0.0.0
  duplex auto
  speed auto
  mpls ip
!
interface CEM0/2
  no ip address
  cem 12
  xconnect 50.0.0.2 3 encapsulation mpls
!
!
interface CEM0/3
  no ip address
  cem 30
  xconnect 50.0.0.2 4 encapsulation mpls
!
interface CEM0/4
  no ip address
  cem 8
  xconnect 50.0.0.2 5 encapsulation mpls
!
!
interface CEM0/5
  no ip address
  cem 25
  xconnect 50.0.0.2 6 encapsulation mpls
!
!
interface ATM0/IMA0
  no ip address
```

```
load-interval 30
mcpt-timers 2000 6000 10000
no ilmi-keepalive
pvc 1/10 l2transport
xconnect 50.0.0.2 101 encapsulation mpls
!
pvc 1/11 l2transport
xconnect 50.0.0.2 102 pw-class mpls
!
pvc 1/21 l2transport
encapsulation aal0
cell-packing 28 mcpt-timer 2
xconnect 50.0.0.2 111 encapsulation mpls
!
pvc 1/22 l2transport
encapsulation aal0
cell-packing 18 mcpt-timer 3
xconnect 50.0.0.2 112 encapsulation mpls
!
!
interface ATM0/IMA0.1 point-to-point
no snmp trap link-status
pvc 1/12 l2transport
xconnect 50.0.0.2 103 encapsulation mpls
!
!
interface ATM0/IMA0.2 multipoint
no snmp trap link-status
cell-packing 20 mcpt-timer 2
xconnect 50.0.0.2 104 pw-class mpls
pvc 1/13 l2transport
encapsulation aal0
!
pvc 1/14 l2transport
encapsulation aal0
!
!
interface ATM0/IMA0.3 point-to-point
no snmp trap link-status
pvc 1/15 l2transport
encapsulation aal0
cell-packing 10 mcpt-timer 3
xconnect 50.0.0.2 105 pw-class mpls
!
!
interface ATM0/IMA0.4 point-to-point
no snmp trap link-status
pvc 1/16 l2transport
encapsulation aal0
cell-packing 14 mcpt-timer 3
xconnect 50.0.0.2 106 pw-class mpls one-to-one
!
interface ATM0/IMA0.6 multipoint
no snmp trap link-status
pvc 1/17 l2transport
xconnect 50.0.0.2 107 pw-class mpls
!
pvc 1/18 l2transport
encapsulation aal0
xconnect 50.0.0.2 108 encapsulation mpls
!
pvc 1/19 l2transport
encapsulation aal0
cell-packing 12 mcpt-timer 1
```

```

    xconnect 50.0.0.2 109 encapsulation mpls
    !
    !
interface ATM1/0
    no ip address
    load-interval 30
    scrambling-payload
    mcpt-timers 1000 5000 10000
    no ilmi-keepalive
    pvc 0/5 l2transport
        encapsulation aal0
        cell-packing 10 mcpt-timer 3
        xconnect 50.0.0.2 10 pw-class l2tp
    !
    pvc 0/6 l2transport
        xconnect 50.0.0.2 20 pw-class l2tp
    !
    pvc 0/7 l2transport
        encapsulation aal0
        cell-packing 28 mcpt-timer 3
        xconnect 50.0.0.2 30 encapsulation mpls pw-class mpls one-to-one
    !
    pvc 0/8 l2transport
        xconnect 50.0.0.2 40 pw-class mpls
    !
    pvc 0/9 l2transport
        encapsulation aal0
        xconnect 50.0.0.2 50 pw-class mpls one-to-one
    !
    !
interface ATM1/0.1 point-to-point
    no snmp trap link-status
    pvc 0/15 l2transport
        xconnect 50.0.0.2 13 pw-class mpls
    !
    !
interface ATM1/0.2 multipoint
    no snmp trap link-status
    cell-packing 2 mcpt-timer 1
    xconnect 50.0.0.2 12 encapsulation mpls
    pvc 0/10 l2transport
        encapsulation aal0
    !
    pvc 0/11 l2transport
        encapsulation aal0
    !
    pvc 0/12 l2transport
        encapsulation aal0
    !
    pvc 0/13 l2transport
        encapsulation aal0
    !
    !
interface ATM1/0.3 point-to-point
    no snmp trap link-status
    pvc 0/16 l2transport
        encapsulation aal0
        xconnect 50.0.0.2 14 encapsulation mpls
    !
    !
interface ATM1/0.4 point-to-point
    no snmp trap link-status
    pvc 0/17 l2transport
        encapsulation aal0

```



```

    xconnect 50.0.0.2 15 pw-class mpls one-to-one
    !
!
interface ATM1/0.6 multipoint
  no snmp trap link-status
  pvc 0/26 l2transport
    xconnect 50.0.0.2 16 pw-class mpls
    !
  pvc 0/27 l2transport
    encapsulation aal0
    cell-packing 8 mcpt-timer 3
    xconnect 50.0.0.2 17 pw-class mpls
    !
  pvc 0/28 l2transport
    encapsulation aal0
    cell-packing 16 mcpt-timer 2
    xconnect 50.0.0.2 18 pw-class mpls
    !
!
interface ATM1/0.7 multipoint
  no snmp trap link-status
  !
interface ATM1/1
  no ip address
  scrambling-payload
  mcpt-timers 1000 5000 10000
  no ilmi-keepalive
  cell-packing 20 mcpt-timer 2
  xconnect 50.0.0.2 11 encapsulation mpls
  pvc 0/21 l2transport
    encapsulation aal0
    !
  pvc 0/22 l2transport
    encapsulation aal0
    !
  pvc 0/23 l2transport
    encapsulation aal0
    !
!
interface ATM1/1.1 point-to-point
  no snmp trap link-status
  !
interface ATM1/1.2 multipoint
  no snmp trap link-status
  !
interface ATM1/2
  no ip address
  scrambling-payload
  ima-group 0
  no ilmi-keepalive
  !
ip route 9.10.0.254 255.255.255.255 9.11.49.254
ip route 30.0.0.0 255.0.0.0 GigabitEthernet0/0
ip route 50.0.0.2 255.255.255.255 20.0.0.2
ip route 50.0.0.5 255.255.255.255 20.0.0.2
!
!
ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback50 force
!
!

```

```
!  
!  
!  
alias exec cpu show proc cpu | i CPU  
alias exec hist show proc cpu history  
alias exec clc clear counters  
alias exec cmpls clear mpls counters  
!  
line con 0  
  exec-timeout 0 0  
line aux 0  
line vty 0 4  
  login  
!  
end
```

## PE\_2

```
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname MWR2  
!  
boot-start-marker  
boot-end-marker  
!  
card type e1 0 0  
card type e1 0 1  
card type e1 0 2  
card type e1 1 0  
card type e1 1 1  
logging buffered 1000000  
enable password lab  
!  
no aaa new-model  
!  
network-clock-select 1 E1 0/0  
network-clock-select 2 E1 0/1  
network-clock-select 3 E1 0/2  
network-clock-select 4 E1 0/3  
network-clock-select 5 E1 0/4  
network-clock-select 6 E1 0/5  
ipran-alt-interrupt tracing  
mmi polling-interval 60  
no mmi auto-configure  
no mmi pvc  
mmi snmp-timeout 180  
ip cef  
!  
!  
no ip domain lookup  
vlan ifdescr detail  
multilink bundle-name authenticated  
mpls label protocol ldp  
vpdn enable  
!  
!  
!  
!  
!  
!
```

```
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
  log config  
!  
!  
controller E1 0/0  
  cem-group 1 unframed  
!  
controller E1 0/1  
  cem-group 20 unframed  
!  
controller E1 0/2  
  cem-group 12 unframed  
!  
controller E1 0/3  
  cem-group 30 unframed  
!  
controller E1 0/4  
  cem-group 8 unframed  
!  
controller E1 0/5  
  cem-group 25 unframed  
!  
controller E1 1/0  
  mode aim 1  
  clock source internal  
!  
controller E1 1/1  
  mode aim 1  
  clock source internal  
!  
controller E1 1/2  
  mode aim 1  
  clock source internal  
!  
controller E1 1/3  
  clock source internal  
!  
pseudowire-class mpls  
  encapsulation mpls  
  preferred-path peer 50.0.0.1  
!  
pseudowire-class l2tp  
  encapsulation l2tpv3  
  ip protocol udp  
  ip local interface Loopback50  
!  
!  
class cem test  
!  
class cem cemclass  
  payload-size 32  
!
```

```

!
!
!
!
!
interface Loopback50
 ip address 50.0.0.2 255.255.255.255
!
interface CEM0/0
 no ip address
 cem 1
 xconnect 50.0.0.1 1 encapsulation mpls
!
!
interface GigabitEthernet0/0
 ip address 30.0.0.1 255.0.0.0
 duplex auto
 speed auto
 mpls ip
!
interface CEM0/1
 no ip address
 cem 20
 xconnect 50.0.0.1 2 encapsulation mpls
!
!
interface GigabitEthernet0/1
 ip address 70.0.0.1 255.0.0.0
 duplex auto
 speed auto
 mpls ip
!
interface CEM0/2
 no ip address
 cem 12
 xconnect 50.0.0.1 3 encapsulation mpls
!
!
interface CEM0/3
 no ip address
 cem 30
 xconnect 50.0.0.1 4 encapsulation mpls
!
!
interface CEM0/4
 no ip address
 cem 8
 xconnect 50.0.0.1 5 encapsulation mpls
!
!
interface CEM0/5
 no ip address
 cem 25
 xconnect 50.0.0.1 6 encapsulation mpls
!
!
interface ATM0/IMA0
 no ip address
 load-interval 30
 mcpt-timers 2000 6000 10000
 no ilmi-keepalive
 pvc 1/10 l2transport
 xconnect 50.0.0.1 101 encapsulation mpls

```

```
!  
pvc 1/11 l2transport  
  xconnect 50.0.0.1 102 pw-class mpls  
!  
pvc 1/21 l2transport  
  encapsulation aal0  
  xconnect 50.0.0.1 111 encapsulation mpls  
!  
pvc 1/22 l2transport  
  encapsulation aal0  
  xconnect 50.0.0.1 112 encapsulation mpls  
!  
!  
interface ATM0/IMA0.1 point-to-point  
  no snmp trap link-status  
  pvc 1/12 l2transport  
    xconnect 50.0.0.1 103 encapsulation mpls  
  !  
!  
interface ATM0/IMA0.2 multipoint  
  no snmp trap link-status  
  cell-packing 15 mcpt-timer 3  
  xconnect 50.0.0.1 104 pw-class mpls  
  pvc 1/13 l2transport  
    encapsulation aal0  
  !  
  pvc 1/14 l2transport  
    encapsulation aal0  
  !  
!  
interface ATM0/IMA0.3 point-to-point  
  no snmp trap link-status  
  pvc 1/15 l2transport  
    encapsulation aal0  
    xconnect 50.0.0.1 105 pw-class mpls  
  !  
!  
interface ATM0/IMA0.4 point-to-point  
  no snmp trap link-status  
  pvc 1/16 l2transport  
    encapsulation aal0  
    cell-packing 7 mcpt-timer 2  
    xconnect 50.0.0.1 106 pw-class mpls one-to-one  
  !  
!  
interface ATM0/IMA0.6 multipoint  
  no snmp trap link-status  
  pvc 1/17 l2transport  
    xconnect 50.0.0.1 107 pw-class mpls  
  !  
  pvc 1/18 l2transport  
    encapsulation aal0  
    xconnect 50.0.0.1 108 encapsulation mpls  
  !  
  pvc 1/19 l2transport  
    encapsulation aal0  
    cell-packing 9 mcpt-timer 3  
    xconnect 50.0.0.1 109 encapsulation mpls  
  !  
!  
interface ATM1/0  
  ip address 1.1.1.2 255.0.0.0  
  load-interval 30  
  scrambling-payload
```

```

mcpt-timers 1000 5000 10000
no ilmi-keepalive
pvc 0/5 l2transport
encapsulation aal0
cell-packing 25 mcpt-timer 3
xconnect 50.0.0.1 10 pw-class l2tp
!
pvc 0/6 l2transport
xconnect 50.0.0.1 20 pw-class l2tp
!
pvc 0/7 l2transport
encapsulation aal0
cell-packing 12 mcpt-timer 2
xconnect 50.0.0.1 30 encapsulation mpls pw-class mpls one-to-one
!
pvc 0/8 l2transport
xconnect 50.0.0.1 40 pw-class mpls
!
pvc 0/9 l2transport
encapsulation aal0
xconnect 50.0.0.1 50 pw-class mpls one-to-one
!
pvc 0/99
protocol ip 1.1.1.1 broadcast
encapsulation aal5snap
!
!
interface ATM1/0.1 point-to-point
no snmp trap link-status
pvc 0/15 l2transport
xconnect 50.0.0.1 13 pw-class mpls
!
!
interface ATM1/0.2 multipoint
no snmp trap link-status
cell-packing 10 mcpt-timer 2
xconnect 50.0.0.1 12 encapsulation mpls
pvc 0/10 l2transport
encapsulation aal0
!
pvc 0/11 l2transport
encapsulation aal0
!
pvc 0/12 l2transport
encapsulation aal0
!
pvc 0/13 l2transport
encapsulation aal0
!
!
interface ATM1/0.3 point-to-point
no snmp trap link-status
pvc 0/16 l2transport
encapsulation aal0
xconnect 50.0.0.1 14 encapsulation mpls
!
!
interface ATM1/0.4 point-to-point
no snmp trap link-status
pvc 0/17 l2transport
encapsulation aal0
xconnect 50.0.0.1 15 pw-class mpls one-to-one
!
!

```

```
interface ATM1/0.6 multipoint
  no snmp trap link-status
  pvc 0/26 l2transport
    xconnect 50.0.0.1 16 pw-class mpls
  !
  pvc 0/27 l2transport
    encapsulation aal0
    cell-packing 18 mcpt-timer 3
    xconnect 50.0.0.1 17 pw-class mpls
  !
  pvc 0/28 l2transport
    encapsulation aal0
    cell-packing 24 mcpt-timer 2
    xconnect 50.0.0.1 18 pw-class mpls
  !
!
interface ATM1/0.7 multipoint
  no snmp trap link-status
!
interface ATM1/1
  no ip address
  scrambling-payload
  mcpt-timers 1000 5000 10000
  no ilmi-keepalive
  cell-packing 20 mcpt-timer 2
  xconnect 50.0.0.1 11 encapsulation mpls
  pvc 0/21 l2transport
    encapsulation aal0
  !
  pvc 0/22 l2transport
    encapsulation aal0
  !
  pvc 0/23 l2transport
    encapsulation aal0
  !
!
interface ATM1/2
  no ip address
  scrambling-payload
  ima-group 0
  no ilmi-keepalive
!
ip route 9.10.0.254 255.255.255.255 9.11.49.254
ip route 20.0.0.0 255.0.0.0 GigabitEthernet0/0
ip route 50.0.0.1 255.255.255.255 70.0.0.2
ip route 50.0.0.5 255.255.255.255 70.0.0.2
!
!
ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback50 force
!
!
!
!
!
alias exec cpu show proc cpu | i CPU
alias exec hist show proc cpu history
alias exec clc clear counters
alias exec cmpls clear mpls counters
!
line con 0
```

**Examples**

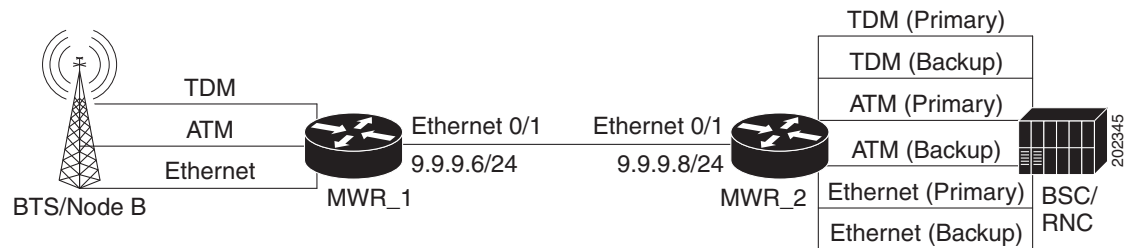
```
exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  login
!
end
```



## PWE3 Redundancy Configuration

The following example shows a PWE3 Redundancy configuration (Figure B-2).

**Figure B-2 PWE3 Redundancy Configuration**



### MWR\_1

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname mwr-pe1
!
boot-start-marker
boot-end-marker
!
card type e1 0 1
card type e1 0 2
card type e1 1 0
card type e1 1 1
logging buffered 10000000
enable password lab
!
no aaa new-model
!
network-clock-select 1 E1 1/2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
!
!
!
no ip domain lookup
vlan ifdescr detail
multilink bundle-name authenticated
mpls label protocol ldp
vpdn enable
!
archive
 log config
  hidekeys
!
!
controller E1 0/0
 clock source internal
 cem-group 0 unframed

```

```

!
controller E1 0/1
!
controller E1 0/2
!
controller E1 0/3
  clock source internal
!
controller E1 1/0
  mode aim 1
  clock source internal
!
controller E1 1/1
!
controller E1 1/2
!
controller E1 1/3
  clock source internal
!
interface cem0/0
  cem 0
  xconnect 2.2.2.2 1 encapsulation mpls
  backup peer 2.2.2.2 2
  backup delay 20 20
!
interface ATM1/0
  no ip address
  scrambling-payload
  no ilmi-keepalive
  xconnect 2.2.2.2 3 encapsulation mpls
  backup peer 2.2.2.2 4
  backup delay 20 20
  pvc 0/1 l2transport
  encapsulation aal0
!
interface Loopback0
  no ip address
!
interface Loopback1
  ip address 1.1.1.1 255.255.255.255
  load-interval 30
!
interface Loopback101
  no ip address
!
!
!
!
interface GigabitEthernet0/0.3
  encapsulation dot1q 3
  xconnect 2.2.2.2 5 encapsulation mpls
  backup peer 2.2.2.2 6
  backup delay 20 20
!
interface GigabitEthernet0/1
  ip address 9.9.9.6 255.255.255.0
  load-interval 30
  speed 100
  full-duplex
  mpls ip
!
!
ip forward-protocol nd
ip route 2.2.2.2 255.255.255.255 9.9.9.8

```

```

!
ip http server
no ip http secure-server
!
!
snmp-server community public RO
!
!
!
control-plane
!
!
!
!
!
!
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  password lab
  login
!
exception data-corruption buffer truncate
!
end

```

## MWR\_2

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname mwr-pe2
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
card type e1 1 0
card type e1 1 1
logging buffered 10000000
enable password lab
!
no aaa new-model
!
network-clock-select 1 E1 0/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip arp proxy disable
ip cef
!
!
!
!

```

```
no ip domain lookup
vlan ifdescr detail
l2tp-class l2tp
multilink bundle-name authenticated
mpls label protocol ldp
mpls ldp session protection
mpls oam
    echo revision 4
vpdn enable
!
!
!
!
archive
    log config
    hidekeys
!
!
controller E1 0/0
    cem-group 0 unframed
!
controller E1 0/1
    clock source internal
    cem-group 0 unframed
!
controller E1 0/2
!
controller E1 0/3
    clock source internal
!
controller E1 0/4
    clock source internal
!
controller E1 0/5
!
controller E1 1/0
    mode aim 1
    clock source internal
!
controller E1 1/1
    clock source internal
!
controller E1 1/2
    clock source internal
!
controller E1 1/3
    mode aim 1
    clock source internal
!
! Primary
interface cem0/0
    cem 0
    xconnect 1.1.1.1 1 encapsulation mpls
!
! Backup
interface cem0/1
    cem 0
    xconnect 1.1.1.1 2 encapsulation mpls
!
! Primary
interface ATM1/0
    no ip address
    scrambling-payload
```

```

no ilmi-keepalive
xconnect 1.1.1.1 3 encapsulation mpls
pvc 0/1 l2transport
    encapsulation aal0
!
! Backup
interface ATM1/3
no ip address
    scrambling-payload
no ilmi-keepalive
xconnect 1.1.1.1 4 encapsulation mpls
pvc 0/1 l2transport
    encapsulation aal0
!
!
interface Loopback1
    ip address 2.2.2.2 255.255.255.255
!

! Primary
interface GigabitEthernet0/0.3
encapsulation dot1q 3
xconnect 1.1.1.1 5 encapsulation mpls
!
! Backup
interface GigabitEthernet0/0.4
encapsulation dot1q 4
xconnect 1.1.1.1 6 encapsulation mpls
!
!
!
interface GigabitEthernet0/1
    ip address 9.9.9.8 255.255.255.0
    load-interval 30
    speed 100
    full-duplex
    mpls ip
    no cdp enable
!
ip forward-protocol nd
ip route 1.1.1.1 255.255.255.255 9.9.9.6
!
no ip http server
no ip http secure-server
!
!
snmp-server community private RW
snmp-server community public RO
snmp-server ifindex persist
snmp-server trap link ietf
no snmp-server sparse-tables
snmp-server queue-length 100
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps ipran
no cdp run
route-map test permit 10
    match mpls-label
!
!
!
mpls ldp router-id Loopback1 force
!
control-plane
!

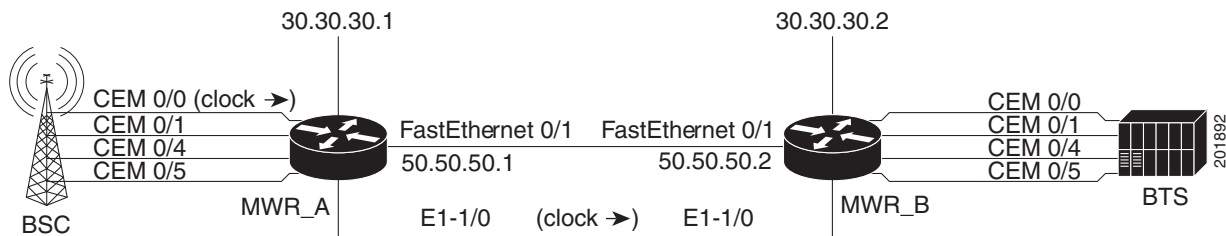
```

```
no call rsvp-sync
!  
!  
!  
line con 0  
  exec-timeout 0 0  
  logging synchronous  
line aux 0  
line vty 0 4  
  exec-timeout 0 0  
  password lab  
  login  
!  
exception data-corruption buffer truncate  
!  
end
```

## TDM over MPLS Configuration

Figure B-3 shows a TDM over MPLS configuration. The configuration uses both SAToP and CESoPSN for E1 and T1.

**Figure B-3** TDM over MPLS Configuration



### MWR\_A

```
!
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service internal
!
hostname mwr_A
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type t1 0 2
enable password xxx
!
no aaa new-model
clock timezone est -5
!
network-clock-select 1 E1 0/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
controller E1 0/0
cem-group 0 timeslots 1-31
description E1 CESoPSN example
!
controller E1 0/1
clock source internal
cem-group 1 unframed
description E1 SAToP example
!
controller T1 0/4
framing esf
clock source internal
linecode b8zs
cem-group 4 unframed
description T1 SAToP example
!
```

```
controller T1 0/5
framing esf
clock source internal
linecode b8zs
cem-group 5 timeslots 1-24
description T1 CESoPSN example
!
controller E1 1/0
clock source internal
!
controller E1 1/1
!
interface Loopback0
ip address 30.30.30.1 255.255.255.255
!
interface CEM0/0
no ip address
cem 0
    xconnect 30.30.30.2 300 encapsulation mpls
!
!
interface GigabitEthernet0/0
duplex auto
speed auto
no cdp enable
!
interface CEM0/1
no ip address
cem 1
    xconnect 30.30.30.2 301 encapsulation mpls
!
!
interface GigabitEthernet0/1
ip address 50.50.50.1 255.255.255.0
duplex auto
speed auto
mpls ip
no cdp enable
!
interface CEM0/4
no ip address
cem 4
    xconnect 30.30.30.2 304 encapsulation mpls
!
!
interface CEM0/5
no ip address
cem 5
    xconnect 30.30.30.2 305 encapsulation mpls
!
!
no ip classless
ip route 30.30.30.2 255.255.255.255 50.50.50.2
!
no ip http server
no ip http secure-server
!
line con 0
password xxx
login
line aux 0
password xxx
login
no exec
```



```
line vty 0 4
password xxx
login
!
end
```

### MWR\_B

```
!
version 12.4
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service internal
!
hostname mwr_B
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type t1 0 2
enable password xxx
!
no aaa new-model
clock timezone est -5
!
network-clock-select 1 E1 1/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
controller E1 0/0
clock source internal
cem-group 0 timeslots 1-31
description E1 CESoPSN example
!
controller E1 0/1
clock source internal
cem-group 1 unframed
description E1 SATOP example
!
controller T1 0/4
framing esf
clock source internal
linecode b8zs
cem-group 4 unframed
description T1 SATOP example
!
controller T1 0/5
framing esf
clock source internal
linecode b8zs
cem-group 5 timeslots 1-24
description T1 CESoPSN example
!
controller E1 1/0

!
controller E1 1/1
!
```

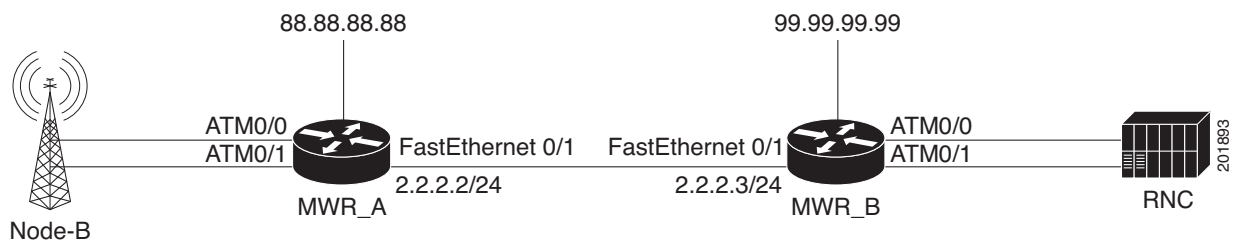
```
interface Loopback0
ip address 30.30.30.2 255.255.255.255
!
interface CEM0/0
no ip address
cem 0
    xconnect 30.30.30.1 300 encapsulation mpls
!
!
interface GigabitEthernet0/0
duplex auto
speed auto
no cdp enable
!
interface CEM0/1
no ip address
cem 1
    xconnect 30.30.30.1 301 encapsulation mpls
!
!
interface GigabitEthernet0/1
ip address 50.50.50.2 255.255.255.0
duplex auto
speed auto
mpls ip
no cdp enable
!
interface CEM0/4
no ip address
cem 4
    xconnect 30.30.30.1 304 encapsulation mpls
!
!
interface CEM0/5
no ip address
cem 5
    xconnect 30.30.30.1 305 encapsulation mpls
!
!
no ip classless
ip route 30.30.30.2 255.255.255.255 50.50.50.1
!
no ip http server
no ip http secure-server
!
line con 0
password xxx
login
line aux 0
password xxx
login
no exec
line vty 0 4
password xxx
login
!
end
```

## ATM over MPLS Configuration

This example shows how to accomplish the following configurations (Figure B-4):

- port mode PW on interface 0/0
- AAL5 SDU mode PW on 0/1 PVC 0/100
- N:1 VCC cell mode PW on 0/1 PVC 0/101
- Multiple PVCs N:1 VCC cell mode PW on 0/1.1
- 1:1 VCC cell mode PW on 0/1 PVC 0/102
- Cell-packing for port mode PWs
- VCC cell-relay mode PWs
- PVC mapping for 0/1.1 N:1 VCC cell relay PWs

**Figure B-4** ATM over MPLS Configuration



### MWR\_A

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname mwr_A
!
boot-start-marker
boot-end-marker
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
card type e1 1 0
logging buffered 4096
enable password lab
!
no aaa new-model
memory-size iomem 25
!
network-clock-select 1 E1 1/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
!
!
no ip domain lookup
```

Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide

```
interface ATM0/0
  no ip address
  scrambling-payload
  mcpt-timers 1000 2000 3000
  no ilmi-keepalive
  cell-packing 28 mcpt-timer 3
  xconnect 99.99.99.99 100 encapsulation mpls
  pvc 1/35 l2transport
    encapsulation aal0
  !
  pvc 1/36 l2transport
    encapsulation aal0
  !
  pvc 1/37 l2transport
    encapsulation aal0
  !
!
interface GigabitEthernet0/0
  ip address 172.18.52.129 255.255.255.0
  duplex auto
  speed auto
  no keepalive
!
interface ATM0/1
  no ip address
  load-interval 30
  scrambling-payload
  mcpt-timers 1000 2000 3000
  no ilmi-keepalive
  pvc 0/10
  !
  pvc 0/100 l2transport
    encapsulation aal5
    xconnect 99.99.99.99 1100 encapsulation mpls
  !
  pvc 0/101 l2transport
    encapsulation aal0
    cell-packing 28 mcpt-timer 3
    xconnect 99.99.99.99 1101 encapsulation mpls
  !
  pvc 0/102 l2transport
    encapsulation aal0
    cell-packing 28 mcpt-timer 3
    xconnect 99.99.99.99 1102 encapsulation mpls
  !
  pvc 0/103 l2transport
    encapsulation aal0
    cell-packing 28 mcpt-timer 3
    xconnect 99.99.99.99 1103 pw-class mpls-exp-5
  !
!
interface ATM0/1.1 multipoint
  no snmp trap link-status
  cell-packing 28 mcpt-timer 3
  xconnect 99.99.99.99 1200 encapsulation mpls
  pvc 1/35 l2transport
    encapsulation aal0
    pw-pvc 2/135
  !
  pvc 1/36 l2transport
    encapsulation aal0
    pw-pvc 2/136
  !
  pvc 1/37 l2transport
```

```
    encapsulation aal0
    pw-pvc 2/137
    !
    !
interface GigabitEthernet0/1
    description interface to 7600 fas 3/5
    ip address 2.2.2.2 255.255.255.0
    duplex auto
    speed auto
    mpls ip
    no keepalive
    !
interface ATM0/2
    no ip address
    scrambling-payload
    no ilmi-keepalive
    !
interface ATM0/3
    no ip address
    scrambling-payload
    no ilmi-keepalive
    !
interface ATM0/IMA1
    no ip address
    no ilmi-keepalive
    !
ip route 0.0.0.0 0.0.0.0 172.18.52.1
ip route 99.99.99.99 255.255.255.255 2.2.2.3
    !
    !
ip http server
no ip http secure-server
    !
    !
mpls ldp router-id Loopback0
disable-eadi
    !
    !
    !
    !
line con 0
    exec-timeout 0 0
line aux 0
line vty 0 4
    exec-timeout 0 0
    privilege level 15
    password lab
    no login
    !
end
```

### MWR\_B

```
    !
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
    !
hostname mwr_B
    !
boot-start-marker
boot-end-marker
    !
```

```
card type e1 0 0  
card type e1 0 1  
logging buffered 4096  
enable password lab  
!  
no aaa new-model  
!  
network-clock-select 1 E1 0/0  
mmi polling-interval 60  
no mmi auto-configure  
no mmi pvc  
mmi snmp-timeout 180  
ip cef  
!  
!  
no ip domain lookup  
ip domain name cisco.com  
multilink bundle-name authenticated  
mpls label protocol ldp  
vpdn enable  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
archive  
    log config  
!  
!  
controller E1 0/0  
    mode aim 1  
!  
controller E1 0/1  
    mode aim 1  
!  
controller E1 0/2  
    mode aim 1  
!  
controller E1 0/3  
    mode aim 1  
!  
controller E1 0/4  
!  
controller E1 0/5  
!  
pseudowire-class mpls-exp-5  
    encapsulation mpls  
    mpls experimental 5  
!  
!  
!
```

```
!  
!  
!  
!  
!  
interface Loopback0  
 ip address 99.99.99.99 255.255.255.255  
!  
interface ATM0/0  
 no ip address  
 scrambling-payload  
  mcpt-timers 1000 2000 3000  
 no ilmi-keepalive  
  cell-packing 28 mcpt-timer 3  
 xconnect 88.88.88.88 100 encapsulation mpls  
 pvc 1/35 l2transport  
  encapsulation aal0  
 !  
 pvc 1/36 l2transport  
  encapsulation aal0  
 !  
 pvc 1/37 l2transport  
  encapsulation aal0  
 !  
 !  
 interface GigabitEthernet0/0  
  ip address 172.18.52.130 255.255.255.0  
  duplex auto  
  speed auto  
  keepalive 1  
 !  
 interface ATM0/1  
  no ip address  
  scrambling-payload  
   mcpt-timers 1000 2000 3000  
  no ilmi-keepalive  
  pvc 0/2  
  !  
  pvc 0/100 l2transport  
   encapsulation aal5  
   xconnect 88.88.88.88 1100 encapsulation mpls  
  !  
  pvc 0/101 l2transport  
   encapsulation aal0  
   cell-packing 28 mcpt-timer 3  
   xconnect 88.88.88.88 1101 encapsulation mpls  
  !  
  pvc 0/102 l2transport  
   encapsulation aal0  
   cell-packing 28 mcpt-timer 3  
   xconnect 88.88.88.88 1102 encapsulation mpls  
  !  
  pvc 0/103 l2transport  
   encapsulation aal0  
   cell-packing 28 mcpt-timer 3  
   xconnect 88.88.88.88 1103 pw-class mpls-exp-5  
  !  
 !  
 interface ATM0/1.1 multipoint  
  no snmp trap link-status  
  cell-packing 28 mcpt-timer 3  
  xconnect 88.88.88.88 1200 encapsulation mpls  
  pvc 2/135 l2transport  
   encapsulation aal0
```

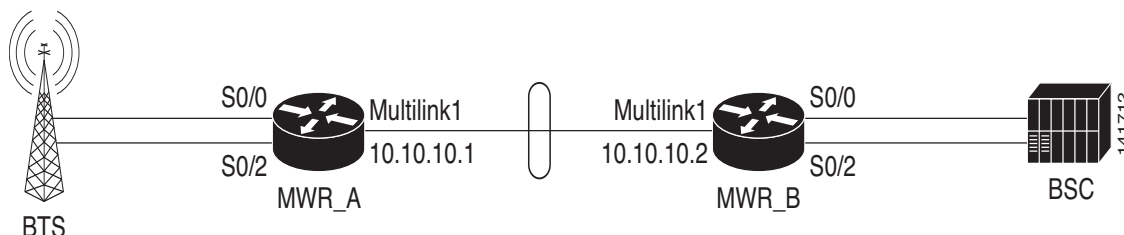


```
!  
pvc 2/136 l2transport  
    encapsulation aal0  
!  
pvc 2/137 l2transport  
    encapsulation aal0  
!  
!  
interface GigabitEthernet0/1  
    ip address 2.2.2.3 255.255.255.0  
    duplex auto  
    speed auto  
    mpls ip  
!  
interface ATM0/2  
    no ip address  
    scrambling-payload  
    ima-group 0  
    no ilmi-keepalive  
!  
interface ATM0/3  
    no ip address  
    scrambling-payload  
    ima-group 0  
    no ilmi-keepalive  
!  
ip route 0.0.0.0 0.0.0.0 172.18.52.1  
ip route 88.88.88.88 255.255.255.255 2.2.2.2  
!  
!  
ip http server  
no ip http secure-server  
!  
!  
mpls ldp router-id Loopback0  
!  
!  
!  
!  
line con 0  
    exec-timeout 0 0  
line aux 0  
line vty 0 4  
    exec-timeout 0 0  
    password lab  
    login  
!  
end
```

## GSM-Only Configuration

The standard GSM topology includes one or more shorthaul interface connections from the BTS to a Cisco MWR 2941-DC through separate T1/E1 connections. The Cisco MWR 2941-DC routers are connected back-to-back using an MLPPP backhaul connection (two or more T1/E1 connections). At the BSC side, the Cisco MWR 2941-DC-to-BSC connectivity is exactly the same as the BTS-to-Cisco MWR 2941-DC connections. In this example, only GSM traffic traverses the topology ([Figure B-5](#)).

**Figure B-5** GSM-Only Configuration



### MWR\_A

```
!
card type E1 0 0
card type E1 0 1
!
network-clock-select 1 E1 0/1
!
ipran-mib snmp-access inBand
ipran-mib location cellSite
!
!
controller E1 0/0
    framing NO-CRC4
    clock source internal
    channel-group 0 timeslots 1-31
!
controller E1 0/1
    channel-group 0 timeslots 1-31
!
controller E1 0/2
    framing NO-CRC4
    clock source internal
    channel-group 0 timeslots 1-31
!
!
class-map match-any llq-class
match ip dscp ef
!
!
policy-map llq-policy
class llq-class
    priority percent 99
class class-default
    bandwidth remaining percent 1
    queue-limit 45
!
interface Multilink1
ip address 10.10.10.1 255.255.255.252
load-interval 30
```

```
no keepalive
no cdp enable
ppp pfc local request
ppp pfc remote apply
ppp acfc local request
ppp acfc remote apply
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
max-reserved-bandwidth 100
service-policy output llq-policy
hold-queue 50 out
ip rtp header-compression ietf-format
!
!
interface Serial0/0:0
no ip address
encapsulation gsm-abis
gsm-abis local 10.10.10.1 4444
gsm-abis remote 10.10.10.2 4444
gsm-abis set dscp ef
no keepalive
!
interface Serial0/1:0
no ip address
encapsulation ppp
keepalive 1
ppp multilink group 1
max-reserved-bandwidth 100
!
interface Serial0/2:0
no ip address
encapsulation gsm-abis
gsm-abis local 10.10.10.1 4446
gsm-abis remote 10.10.10.2 4446
gsm-abis set dscp ef
no keepalive
!
logging history size 500
logging history debugging
logging trap warnings
snmp-server community public RO
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
snmp-server enable traps syslog
snmp-server trap link ietf
snmp-server ifIndex persist
no snmp-server sparse-table
snmp-server host 64.50.100.254 version 2c V2C
disable-eadi
```

## MWR\_B

```
!
card type E1 0 0
card type E1 0 1
!
network-clock-select 1 E1 0/0
network-clock-select 2 E1 0/2
!
ipran-mib snmp-access outOfBand
```

```

ipran-mib location aggSite
!
!
controller E1 0/0
    framing NO-CRC4
    channel-group 0 timeslots 1-31
!
controller E1 0/1
    clock source internal
    channel-group 0 timeslots 1-31
!
controller E1 0/2
    framing NO-CRC4
    channel-group 0 timeslots 1-31
!
!
class-map match-any llq-class
match ip dscp ef
!
!
policy-map llq-policy
class llq-class
    priority percent 99
class class-default
    bandwidth remaining percent 1
    queue-limit 45
!
interface Multilink1
ip address 10.10.10.2 255.255.255.252
load-interval 30
no keepalive
no cdp enable
ppp pfc local request
ppp pfc remote apply
ppp acfc local request
ppp acfc remote apply
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
max-reserved-bandwidth 100
service-policy output llq-policy
hold-queue 50 out
ip rtp header-compression ietf-format
!
!
interface Serial0/0:0
no ip address
encapsulation gsm-abis
gsm-abis local 10.10.10.2 4444
gsm-abis remote 10.10.10.1 4444
gsm-abis set dscp ef
no keepalive
!
interface Serial0/1:0
no ip address
encapsulation ppp
keepalive 1
ppp multilink group 1
max-reserved-bandwidth 100
!
interface Serial0/2:0
no ip address

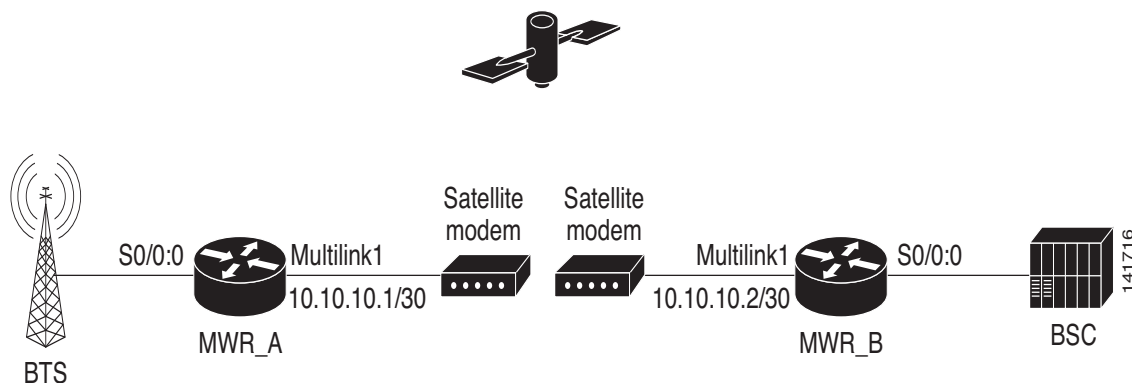
```

```
encapsulation gsm-abis
gsm-abis local 10.10.10.2 4446
gsm-abis remote 10.10.10.1 4446
gsm-abis set dscp ef
no keepalive
!
logging history size 500
logging history debugging
logging trap warnings
snmp-server community public RO
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
snmp-server enable traps syslog
snmp-server trap link ietf
snmp-server ifIndex persist
no snmp-server sparse-table
snmp-server host 64.50.100.254 version 2c V2C
disable-eadi
```

## GSM-Only Configuration Using Satellite

The GSM-only using satellite configuration allows for point-to-point network optimization (Figure B-6).

**Figure B-6** GSM-Only Configuration Using Satellite



### MWR\_A

```
!
card type E1 0 0
!
network-clock-select 1 E1 0/1
!
ipran-mib snmp-access inBand
ipran-mib location cellSite
!
!
controller E1 0/0
    framing NO-CRC4
    clock source internal
    channel-group 0 timeslots 1-20
!
controller E1 0/1
    channel-group 0 timeslots 1-20
!
!
class-map match-any llq-class
match ip dscp ef
!
!
policy-map llq-policy
class llq-class
    priority percent 99
class class-default
    bandwidth remaining percent 1
    queue-limit 45
!
interface Multilink1
ip address 10.10.10.1 255.255.255.252
load-interval 30
no keepalive
no cdp enable
ppp pfc local request
ppp pfc remote apply
ppp acfc local request
```

```
ppp acfc remote apply
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
max-reserved-bandwidth 100
service-policy output llq-policy
hold-queue 50 out
ip rtp header-compression ietf-format
!
!
interface Serial0/0:0
no ip address
encapsulation gsm-abis
gsm-abis local 10.10.10.1 4444
gsm-abis remote 10.10.10.2 4444
gsm-abis set dscp ef
no keepalive
!
interface Serial0/1:0
no ip address
encapsulation ppp
keepalive 1
ppp multilink group 1
max-reserved-bandwidth 100
!
logging history size 500
logging history debugging
logging trap warnings
snmp-server community public RO
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
snmp-server enable traps syslog
snmp-server trap link ietf
snmp-server ifIndex persist
no snmp-server sparse-table
snmp-server host 64.50.100.254 version 2c V2C
disable-eadi
```

#### MWR\_B

```
!
card type E1 0 0
!
network-clock-select 1 E1 0/0
```

```

!
ipran-mib snmp-access outOfBand
ipran-mib location aggSite
!
!
controller E1 0/0
    framing NO-CRC4
    channel-group 0 timeslots 1-20
!
controller E1 0/1
    clock source internal
    channel-group 0 timeslots 1-20
!
!
class-map match-any llq-class
match ip dscp ef
!
!
policy-map llq-policy
class llq-class
    priority percent 99
class class-default
    bandwidth remaining percent 1
    queue-limit 45
!
interface Multilink1
ip address 10.10.10.2 255.255.255.252
load-interval 30
no keepalive
no cdp enable
ppp pfc local request
ppp pfc remote apply
ppp acfc local request
ppp acfc remote apply
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
max-reserved-bandwidth 100
service-policy output llq-policy
hold-queue 50 out
ip rtp header-compression ietf-format
!
!
interface Serial0/0:0
no ip address
encapsulation gsm-abis
gsm-abis local 10.10.10.2 4444
gsm-abis remote 10.10.10.1 4444
gsm-abis set dscp ef
no keepalive
!
interface Serial0/1:0
no ip address
encapsulation ppp
keepalive 1
ppp multilink group 1
max-reserved-bandwidth 100
!
logging history size 500
logging history debugging
logging trap warnings
snmp-server community public RO

```



```
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
snmp-server enable traps syslog
snmp-server trap link ietf
snmp-server ifIndex persist
no snmp-server sparse-table
snmp-server host 64.50.100.254 version 2c V2C
disable-eadi
```

## GSM Congestion Management

These examples show how to configure GSM congestion management for the BTS side and the BSC side.

### BTS side

```
interface Serial0/0:0
no ip address
encapsulation gsm-abis
gsm-abis local 10.10.10.1 4444
gsm-abis remote 10.10.10.2 4444
gsm-abis congestion enable
gsm-abis congestion critical 1-10
gsm-abis congestion critical 31
gsm-abis set dscp ef
no keepalive
```

### BSC side

```
interface Serial0/0:0
no ip address
encapsulation gsm-abis
gsm-abis local 10.10.10.2 4444
gsm-abis remote 10.10.10.1 4444
gsm-abis congestion enable
gsm-abis congestion critical 1-10
gsm-abis congestion critical 31
gsm-abis set dscp ef
no keepalive
```





## INDEX

---

### A

ATM port [4-6](#)  
attachment circuits [1-3](#)  
autodiscovery [4-46](#)  
auxiliary port [3-2](#)

---

### B

base station controller  
    *See* BSC  
base station controller (BSC) [4-6](#)  
base transceiver station  
    *See* BTS  
before starting router [3-3](#)  
BSC  
    in RAN [1-1](#)  
BTS  
    in RAN [1-1](#)

---

### C

circuit emulation service over packet-switched network [1-3](#)  
Cisco IOS  
    about [2-1](#)  
    command modes [2-1](#)  
    enable mode [2-2, 4-46](#)  
    help [2-1](#)  
    saving configuration changes [2-3](#)  
    undo command [2-2](#)  
    undo feature [2-2](#)  
CISCO-IP-RAN-BACKHAUL-MIB

    configuration statements [1-7](#)  
Cisco MWR 2941-DC router  
    monitoring and managing [4-46](#)  
    port numbering [3-2](#)  
    show commands for monitoring [4-48](#)  
    slot numbering [3-2](#)  
    understanding interface numbering [3-1](#)  
Cisco Pseudowire Emulation Edge-to-Edge  
    *See* PWE3  
Cisco pseudowire emulation edge-to-edge  
    *See* PWE3  
clocking  
    clocking example (figure) [4-6](#)  
clock signal [4-6](#)  
command line interface  
    *See* CLI  
command modes  
    global configuration [2-2](#)  
    interface configuration [2-2](#)  
    privileged EXEC [2-2](#)  
    user EXEC [2-2](#)  
commands  
    backup delay [A-4](#)  
    backup peer [A-6](#)  
    boot [3-4](#)  
    cdp enable [A-8](#)  
    cem-group [A-9](#)  
    class cem [A-11](#)  
    clear gsm-abis [A-13](#)  
    clear ip rtp header-compression [A-14](#)  
    copy running-config [2-3](#)  
    de jitter-buffer [A-15](#)  
    gsm-abis congestion abate [A-16](#)

- gsm-abis congestion critical [A-17](#)
- gsm-abis congestion enable [A-18](#)
- gsm-abis congestion onset [A-19](#)
- gsm-abis jitter [A-20](#)
- gsm-abis local [A-22](#)
- gsm-abis remote [A-24](#)
- gsm-abis retransmit [A-25](#)
- gsm-abis set dscp [A-26](#)
- help [2-1](#)
- idle-pattern [A-27](#)
- ima-group [A-28](#)
- interface atm ima [A-29](#)
- ip local interface [A-30](#)
- ipran-mib backhaul-notify-interval [A-38](#)
- ipran-mib location [A-40](#)
- ipran-mib snmp-access [A-41](#)
- ipran-mib threshold-acceptable [A-42](#)
- ipran-mib threshold-overloaded [A-43](#)
- ipran-mib threshold-warning [A-44](#)
- ip rtp header-compression [A-32](#)
- ip tcp header-compression [A-35](#)
- keepalive [A-45](#)
- load-interval [A-47](#)
- match ip dscp [A-49](#)
- mpls ip [A-51, A-67, A-69, A-70](#)
- pseudowire-class [A-59](#)
- pw-pvc [A-77](#)
- sample-rate [A-57](#)
- setup [3-3](#)
- show atm cell-packing [A-81](#)
- show cem circuit [A-82](#)
- show cem platform [A-84](#)
- show connection [A-86](#)
- show controller [A-88](#)
- show gsm-abis efficiency [A-90](#)
- show gsm-abis errors [A-93](#)
- show gsm-abis packets [A-95](#)
- show gsm-abis peering [A-96](#)
- show gsm-abis traffic [A-98](#)
- show ip rtp header-compression [A-100](#)
- show mpls l2transport vc [A-102](#)
- show version [4-1](#)
- show xconnect all [A-114](#)
- snmp-server enable traps ipran [A-117](#)
- snmp-server enable traps ipran alarm-gsm [A-118](#)
- snmp-server enable traps ipran util [A-119](#)
- undo [2-2](#)
- xconnect [A-121](#)
- xconnect logging redundancy [A-124](#)
- configuration
  - before starting router [3-3](#)
  - completing [3-6](#)
  - first-time [3-1](#)
  - saving [2-3, 3-6, 4-45](#)
- configuration statements for CISCO-IP-RAN-BACKHAUL-MIB [1-7](#)
- configuring
  - controllers
    - E1 interface [4-23](#)
  - for SNMP support [4-33](#)
  - GE interfaces [4-4](#)
  - global parameters [3-3](#)
  - gsm-abis congestion critical [A-17](#)
  - gsm-abis congestion onset [A-19](#)
  - gsm-abis jitter [A-20](#)
  - GSM-Abis links [4-31](#)
  - gsm-abis local [A-22](#)
  - gsm-abis remote [A-24](#)
  - hostname [4-2](#)
  - IP address [4-4](#)
  - multilink interface [4-22](#)
  - password [4-2](#)
- console port [3-2](#)
- controllers
  - E1 configuration [4-23](#)

---

**D**

data bearer traffic [1-6](#)  
 duplex mode, setting [4-5](#)

---

**E**

E1 controllers [4-23](#)  
 enable mode [2-2, 4-46](#)  
 event monitoring [4-46](#)

---

**F**

figure  
     asymmetric PWE3 configuration [B-2](#)  
     ATM over MPLS configuration [B-25](#)  
     Cisco MWR 2941-DC router in a cell site POP [1-6](#)  
     Cisco MWR 2941-DC router in a GSM Abis  
     Optimization over IP [1-4](#)  
     Cisco MWR 2941-DC router in a PWE3 [1-2](#)  
     clocking example [4-6](#)  
     GSM only configuration [B-32](#)  
     GSM only configuration through satellite [B-36](#)  
     PWE3 redundancy configuration [B-15](#)  
     TDM over MPLS configuration [B-21](#)  
 first-time configuration [3-1](#)

---

**G**

GE interface  
     configuring [4-4](#)  
     IP address [4-4](#)  
     mode [4-5](#)  
     speed [4-5](#)  
 global parameters  
     configuring [3-3](#)  
 GSM Abis  
     example of Cisco MWR 2941-DC router in a GSM  
     Abis Iub optimization over IP (figure) [1-4](#)

gsm-abis congestion abate  
     set [A-16](#)  
 gsm-abis congestion critical  
     configure [A-17](#)  
 gsm-abis congestion onset  
     configure [A-19](#)  
 gsm-abis jitter  
     configure [A-20](#)  
 GSM-Abis links  
     configuring [4-31](#)  
 gsm-abis local  
     configure [A-22](#)  
 gsm-abis remote  
     configure [A-24](#)

---

**H**

help, Cisco IOS [2-1](#)  
 hostname  
     configuring [4-2](#)  
     verifying [4-3](#)

---

**I**

intelligent cell site IP services [1-5](#)  
 interface  
     configuring E1 [4-23](#)  
     GE, configuring [4-4](#)  
     multilink [4-22](#)  
 IOS software  
     basics [2-1](#)  
     verifying version [4-1](#)  
 IP address  
     configuring [4-4](#)  
     GE interface [4-4](#)

---

**M**

MIB support [1-11](#)

mobile switching center

*See* MSC

monitoring and managing the Cisco MWR 2941-DC router [4-46](#)

MSC

in a RAN [1-1](#)

multilink interface

configuring [4-22](#)

---

**N**

Network-Clock-Participate [A-53](#)

network-clock-select [A-53](#)

---

**P**

password [3-5](#)

configuring [4-2](#)

verifying [4-3](#)

point-of-presence

*See* POP

POP

cell site POP [1-5](#)

example of Cisco MWR 2941-DC router in a cell site POP (figure) [1-6](#)

port numbering

Cisco MWR 2941-DC router [3-2](#)

provider edge [1-3](#)

pseudowire-class [A-59](#)

ptp announce [A-61](#)

ptp clock-destination [A-64](#)

ptp clock-source [A-63](#)

ptp delay-req [A-65](#)

ptp master [A-69](#)

ptp mode [A-70](#)

ptp priority1 [A-71](#)

ptp slave [A-73](#)

ptp sync [A-65](#), [A-74](#)

ptp sync limit [A-76](#)

PWE3

example of asymmetric PWE3 configuration [B-2](#)

example of Cisco MWR 2941-DC router in a PWE3 (figure) [1-2](#)

example of PWE3 redundancy configuration [B-15](#)

overview [1-2](#)

---

**R**

RAN, using the Cisco MWR 2941-DC router [1-1](#)

RAN-O

abis and iub optimization over IP [1-4](#)

implementation [1-6](#)

RAN-optimization

*See* RAN-O

recovered-clock slave [A-78](#)

RNC

in a RAN [1-1](#)

---

**S**

SAToP [1-3](#)

saving configuration changes [2-3](#), [4-45](#)

security [4-46](#)

serial port [4-6](#)

set network-clocks [A-80](#)

setup command facility [3-3](#)

show atm cell-packing [A-81](#)

show commands for monitoring the Cisco MWR 2941-DC router [4-48](#)

show controller [A-88](#)

show controller rtm [A-90](#)

show interface switchport backup [A-99](#)

show network-clocks [A-107](#)

show platform hardware rtm [A-108](#)

show ptp clock [A-109](#)

- show ptp foreign-master-record [A-110](#)
- show ptp parent [A-111](#)
- show ptp port [A-112](#)
- show ptp time-property [A-113](#)
- signaling traffic [1-6](#)
- slot numbering
  - Cisco MWR 2941-DC router [3-2](#)
- SNMP support
  - configuring [4-33](#)
- software
  - IOS basics [2-1](#)
  - verifying version [4-1](#)
- speed, setting [4-5](#)
- Structure-agnostic TDM over Packet [1-3](#)
- Structure-agnostic TDM over Packet (SaToP) [1-3](#)
- switchport backup interface [A-120](#)
- synchronized network operation [4-6](#)

---

## T

- transmit clock [4-6](#)

---

## U

- undo feature
  - Cisco IOS [2-2](#)

---

## V

- verifying
  - hostname [4-3](#)
  - password [4-3](#)
  - software version [4-1](#)
  - version of Cisco IOS software [4-1](#)

---

## W

- web-based reporting [4-46](#)

