Cisco ONS 15454 RAN Service Module Software Configuration Guide

April 27, 2007

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-11910-02

Cisco ONS 15454 RAN Service Module Software Configuration Guide

CONTENTS

INDEX

Preface

This preface describes the objectives, audience, organization, and conventions of this *software configuration guide*.

This preface contains the following sections:

Document Revision History

The Document Revision History table below records technical changes to this document. The table shows the document revision number for the change, the date of the change, and a brief summary of the change. Note that not all Cisco documents use a Document Revision History table.

Revision	Date	Change Summary
OL-11910-02	April 27, 2007	Modified caveat, configuration, and command information.
OL-11910-01	November 20, 2006	This is the first release of this guide.

Objectives

This guide explains how to configure features that enable the Cisco RAN Service Module to be implemented in a radio access network optimization (RAN-O).

Audience

This publication is designed for the person who will be 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 internet working, 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	Overview of the Cisco RAN Service Module	Describes the purpose of the Cisco RAN Service Module r and its unique software features.
Chapter 2	Cisco IOS Software Basics	Describes what you need to know about the Cisco IOS software.
Chapter 3	First-Time Configuration	Describes how to use the setup command facility to configure basic attributes of your router.
Chapter 4	Configuring the Cisco RAN Service Module with the Command-Line Interface	Describes how to use the Cisco IOS software command-line interface (CLI) to configure basic router functionality in an RAN-O.

Chapter	Title	Description
Appendix A	Cisco RAN Service Module Command Reference	Provides information about new and changed commands.
Appendix B	Configuration Examples	Provides examples of configurations.

Conventions

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

Convention	Description
boldface font	Commands and keywords.
italic font	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.
`boldface screen font`	Examples of information you must enter.
< >	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

Use this document with the following guides:

- Cisco ONS 15454-SDH Documents

  - *Cisco ONS 15454-SDH Hardware Installation Guide*
  - *Cisco ONS 15454-SDH Software Configuration Guide*
  - *Regulatory Compliance and Safety Information for the Cisco ONS 15454-SDH*
- Cisco Network Modules Installation Guides
  - *Network Modules Quick Start Guide*
- Cisco Network Modules Installation Guides
  - *Network Modules Quick Start Guide*
  - *Cisco Network Modules Hardware Installation Guide*
- Release Notes

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

Overview of the Cisco RAN Service Module

The Cisco ONS 15454 RAN Service Module implements the aggregation node functionality with the Cisco RAN-O solution. Installed in the Cisco ONS 15454, the Cisco RAN Service Module transmits and receives E1 data steams (for Abis) and OC-3 data streams (for UMTS) via the cross-connect cards.

This chapter includes the following sections:

Introduction

Cisco IOS 12.2(29)SM introduces support for GSM and UMTS Radio Access Network (RAN) Optimization for mobile wireless service providers for the RAN Service Module (ONS-RAN-SVC) on a Cisco ONS 15454 platform. Cisco IOS 12.2(29)SM provides GSM and UMTS RAN Optimization (RAN-O) technology that can extend an IP network to every base station site in the mobile network with a shared backhaul transport, plus optimization to reduce bandwidth requirements.

In RAN Optimization (RAN-O), the Cisco MWR 1941-DC-A router extends IP connectivity to the cell site and the BTS/Node B. 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/Node B and leased line termination and the Cisco ONS 15454 aggregation node via compression (cRTP/cUDP) and packet multiplexing (Multilink PPP).

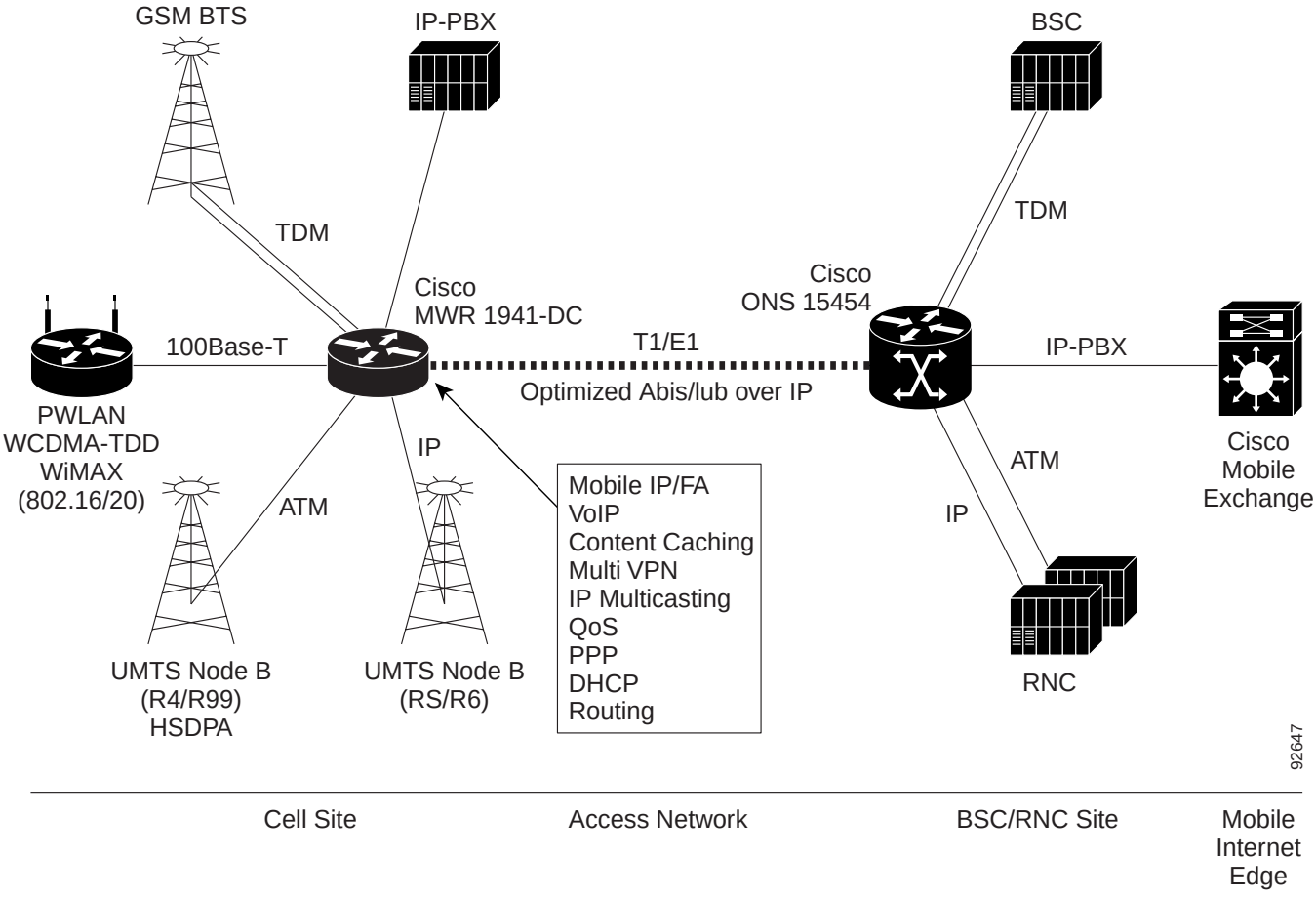
Residing in a Cisco ONS 15454, the Cisco RAN Service Module provides aggregation for traffic originating from multiple MWR cell site routers. The RAN Service Module transmits and receives short haul DS0 level data steams (for GSM applications) and shorthaul VC-4 level data streams (for UMTS applications) through ONS 15454 cross-connect cards. DS0 level channel cards connect both the long haul to the remote cell site and the short haul to GSM BSC. Clear channel VC-4 level interface cards are used on the Cisco ONS 15454 to provide the interface from the UMTS RNC to the ONS RAN Service Module.

The Cisco RAN Service Module consists of four independent IOS processors. Each Cisco RAN Service Module has four 10/100/1000 Gigabit Ethernet (RJ-45) ports with one port connected to each IOS processor. The Cisco RAN Service Module is also equipped with four VC-4 level Packet over SONET (POS) interfaces and four VC-4 level ATM interfaces. The DSO are maped with a maximum of 126 DSO/E1 interfaces that are distributed among the traffic CPUs for backhaul and shorthaul interfaces depending upon the application. We support a maximum of 96 for GSM-ABIS shorthaul interfaces and a maximum of 48 HDLC/PPP/backhaul interfaces

One IOS processor is dedicated as a service processor while the remaining three IOS processors are dedicated as traffic processors. The Cisco ONS RAN Service Module also includes two RJ-45 ports, one used as a DCE console (labeled Console) and the other used as a debug port (covered with a tab plate).

The Cisco ONS 15454 shelf assembly has 17 card slots that are numbered sequentially from left to right. Slots 1 – 4 and 14 – 17 are multispeed slots. Slots 5, 6, 12 and 13 are high-speed slots. Slots 7 and 11 are dedicated to TCC-I cards. Slots 8 and 10 are dedicated to cross-connect (XC10G) cards. Slot 9 is dedicated to the AIC card. The Cisco ONS RAN Service Module can be installed in Slots 1 through 6 or 12 through 17 depending on the application and line card configuration.

Figure 1 Example of Cisco MWR 1941-DC-A and Cisco ONS 15454 in a Cell Site POP



Features of IOS Release 12.2(29)SM for the RAN Service Module

The following support features are provided by Cisco IOS Release 12.2(29)SM:

- Support for 1:N protection
- Support for SNMP versions 1 and 2c
- Support for standard ONS MIBS and IOS MIBS
- Support for the CISCO-IP-RAN-Backhaul_MIb
- Support for GSM and UMTS RAN Optimization

Limitations, Restrictions, and Important Notes

Unsupported Cisco IOS Software Features

The Cisco ONS RAN Service Module requires a special version of Cisco IOS software. Not all Cisco IOS software features can be used as the core routing is handled by the network processor. The following standard Cisco IOS software features are not supported:

- MPLS
- 802.1Q VLANs
- Frame Relay (FR)

Management Software

To manage the Cisco RAN Service Module with network management software, an IP address must be configured on the GigE port associated with the service CPU of the RAN Service Module so that this IP address can be reached by the network management server.

Redundancy Support

There is no IOS configuration to be configured on the Cisco RAN Service Module. The redundancy support for the RAN Service Module 1:N, and it is configured from CTC. The configuration on the CTC can have either one protection group with one protect card and up to seven working cards, or it can have two protection groups with one protect card and up to four working cards in each group. The revertive timer can be disabled for the Cisco RAN Service Module so a user can manually switch back during a maintenance window.

The IOS configuration on the protect card should not be modified because the protect card needs to have a clean configuration to be ready to pick up the configuration from any of the working cards in the protection group when needed.

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:

Understanding this information will save you time as you begin to use the CLI. If you have never used the Cisco IOS software or if you need a refresher, read this chapter before you proceed to Chapter 3, "First-Time Configuration."

If you are already familiar with the Cisco IOS software, proceed 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. Table 2-1 lists the most common command modes.

Table 2-1 Common Command Modes

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

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 wrong 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

You must enter the **copy running-config startup-config** command to save your configuration changes to NVRAM, so that the changes are not lost if there is a system reload or power outage. 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#
```

Where to Go Next

Now that you know some Cisco IOS software basics, you can begin to configure the router by using the CLI.

Remember the following:

- You can use the question mark (?) and arrow keys to help you enter commands.
- Each command mode restricts you to a set of commands. If you have difficulty entering a command, check the prompt and then enter the question mark (**?**) to see a list of available commands. You might be in the wrong command mode or be using the incorrect syntax.
- To disable a feature, enter the keyword **no** before the command; for example, **no ip routing**.
- You need to save your configuration changes to NVRAM so that the changes are not lost if there is a system reload or power outage.

Proceed to Chapter 3, “First-Time Configuration.” for first time configuration. Otherwise, proceed to Chapter 4, “Configuring the Cisco RAN Service Module with the Command-Line Interface,” to begin configuring the router.

CHAPTER 3

First-Time Configuration

This chapter contains information with which you should be familiar before you begin to configure your Cisco RAN Service Module for the first time.

Understanding the Cisco RAN Service Module Interfaces

The Cisco RAN Service Module is supported in the Cisco ONS 15454 chassis as one of its interface cards.

The Cisco ONS 15454 SDH shelf assembly has 17 card slots that are numbered sequentially from left to right. Slots 1 – 4 and 14 – 17 are multispeed slots. Slots 5, 6, 12 and 13 are high-speed slots. Slots 7 and 11 are dedicated to TCC-I cards. Slots 8 and 10 are dedicated to cross-connect (XC10G) cards. Slots 3 and 15 can host E1N-14 and DS3i-N-12 cards that are used in 1:N protection. Typically, the Cisco RAN Service Module slides into Slots 5, 6 and 12, 13 and connects directly to the backplane power and communications. Slots 5 and 12 would typically hold the working or active RAN Service Module while Slots 6 and 13 would hold a protect or standby RAN Service Module.

In the Cisco ONS 15454 SDH, the Cisco E1-42 cards are used to connect both the long haul E1 to the remote cell site and also the short haul E1 to the BSCs/RNCs. The Cisco ONS 15454 RAN Service Module transmits and receives E1 data streams (for GSM applications) and OC-3 data streams (for UMTS applications) via the Cross Connect cards. For E1 connections (GSM and/or backhaul), as many as 126 E1 interfaces from multiple E1-42 cards may be groomed by the Cross Connect card to form two STM-1 data streams which are directed to and terminated on the Cisco RAN Service Module. For OC-3 interfaces (Packet of SONET [POS] and/or ATM), as many as eight OC-3 interfaces from multiple OC-3 cards may be groomed by the Cross Connect card to form two STM-4 data streams which are directed to and terminated on the Cisco RAN Service Module as well.

Each Service Module has four 10/100/1000 Ethernet MAC IEEE 802.3 specification (RJ-45) ports). The Cisco ONS 15454 RAN Service Module also includes two RJ-45 ports, one used as a DCE console (labeled Console) and the other used as a debug port (covered with a tab plate),

There are four CPUs on the RAN Service Module card. One of these CPUs serves as a service CPU and the other three CPUs are traffic controller CPUs. Each IOS processor is equipped with one front-side 10/100/1000 Gigabit Ethernet port, four OC-3 Packet over SONET (POS) or STM-1 backplane interfaces and 42 E1 backplane interfaces. The RAN Service Module interacts with the rest of the I/O interface cards in the Cisco ONS 15454 chassis through cross connect cards.

The Cisco RAN Service Module has the following traffic interfaces:

- Four Gigabit Ethernet (GigE) interfaces: These interfaces are numbered GigE 0/0, GigE 1/0, GigE 2/0, and GigE 3/0. Each of these interfaces is assigned to one CPU. Interface GigE 0/0 is used for management traffic. The other GigE interfaces (GigE 1/0, GigE 2/0, and GigE 3/0) are used for backhaul communications. These interfaces do not interact with other I/O cards via the cross-connect, but rather are physical ports available on the faceplate of the RAN Service Module.
- Four POS interfaces: These interfaces are POS 0/0, POS 1/0, POS 2/0, and POS 3/0. Each interface resides on one CPU. Interface POS 0/0 is connected to the service CPU and it may be used for management traffic. The other POS interfaces are used for backhaul communications. These interfaces support HDLC and PPP encapsulation. In CTC, the POS interfaces are listed as STM-1 ports 5-8, and they can be cross-connected to other interface cards.
- Four ATM interfaces: Each CPU is equipped with its own ATM interface. Interface ATM0/0 is attached to the service CPU. And interfaces ATM1/0, ATM2/0, and ATM3/0 are connected to traffic CPUs 1, 2, and 3 respectively. These ATM interfaces are not directly accessible via CTC. They must first be assigned to one of four VC4 ports using an IOS-based cross-connect feature which is configured on the RAN Service Module itself. The 4 VC4 ports are listed as STM-1 ports 1-4 in the CTC card view. The IOS based cross-connect feature is described more fully in the section "Configuring the IOS Based Cross-connect.

Note ATM interfaces on the RAN-SVC module support a maximum MTU of 4064. This differs with some other Cisco devices as well as other vendors equipment. IP equipment directly connected to the RAN-SVC ATM interfaces should set their MTU to 4064 for optimum operation.

- 126 E1/T1 interfaces: There are 42 of these interfaces assigned to each of the three traffic CPUs. The interface correspond to cross connect ports 9 through 134. The E1/T1interfaces serve as GSM-abis and backhaul (HDLC/PPP) connections. Users can configure up to 80 GSM-abis interfaces and 40 HDLC/PPP interfaces. No fractional E1/T1 is supported on the Cisco RAN Service Module, All time slots must be configured in a channel group.

Note See the *Cisco ONS 15454 SDH Installation and Operations Guide* for proper installation of the RAN Service Module and other Cisco ONS 15454 cards.

CHAPTER 4

Configuring the Cisco RAN Service Module with the Command-Line Interface

This chapter describes how to use the Cisco IOS software command-line interface (CLI) to configure the the Cisco RAN Service Module and includes the following sections:

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 came 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 product, return to Chapter 2 and read it now. The chapter contains important information that you need to successfully configure your Cisco RAN Service Module.

Before You Begin

Before you configure the Cisco RAN Service Module, make sure the Cisco ONS 15454 platform is equipped with a proper software package and adequate hardware and interface cards. The software package release for the Cisco ONS 15454 should be at least 07.20-M06K-22.90 and up. And Cisco IOS release 12.2(29)SM, ransvc-ipran-mz image, must be installed on the Cisco RAN Service Module.

Verifying the Version of Cisco IOS Software

To implement the Cisco RAN Service Module in a RAN-O solution, Cisco IOS Release 12.2(29)SM must be installed on the Cisco ONS 15454. 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.

RAN Service Module Overview

The Cisco RAN Service Module is supported in the Cisco ONS 15454 chassis as one of the interface cards. There are four CPUs on the RAN Service Module card. One of these CPUs serves as a service CPU and the other three are traffic CPUs. The RAN Service Module interacts with the rest of the I/O interface cards in the Cisco ONS 15454 chassis through cross connect cards. The Cisco RAN Service Module has the following traffic interfaces:

- Four Gigabit Ethernet (GigE) interfaces: These interfaces are numbered GigE 0/0, GigE 1/0, GigE 2/0, and GigE 3/0. Each of these interfaces is assigned to one CPU. Interface GigE 0/0 is used for management traffic. The other GigE interfaces (GigE 1/0, GigE 2/0, and GigE 3/0) are used for backhaul communications. These interfaces do not interact with other I/O cards via the cross-connect, but rather are physical ports available on the faceplate of the RAN Service Module.
- Four POS interfaces: These interfaces are POS 0/0, POS 1/0, POS 2/0, and POS 3/0. Each interface resides on one CPU. Interface POS 0/0 is connected to the service CPU and it may be used for management traffic. The other POS interfaces are used for backhaul communications. These interfaces support HDLC and PPP encapsulation. In CTC, the POS interfaces are listed as STM-1 ports 5-8, and they can be cross-connected to other interface cards.
- Four ATM interfaces: Each CPU is equipped with its own ATM interface. Interface ATM0/0 is attached to the service CPU. And interfaces ATM1/0, ATM2/0, and ATM3/0 are connected to traffic CPUs 1, 2, and 3 respectively. These ATM interfaces are not directly accessible via CTC. They must first be assigned to one of four VC4 ports using an IOS-based cross-connect feature which is configured on the RAN Service Module itself. The 4 VC4 ports are listed as STM-1 ports 1-4 in the CTC card view. The IOS based cross-connect feature is described more fully in the section "Configuring the IOS Based Cross-connect.

- 126 E1/T1 interfaces: There are 42 of these interfaces assigned to each of the three traffic CPUs. The interface correspond to cross connect ports 9 through 134. The E1/T1interfaces serve as GSM-abis and backhaul (HDLC/PPP) connections. Users can configure up to 80 GSM-abis interfaces and 40 HDLC/PPP interfaces. No fractional E1/T1 is supported on the Cisco RAN Service Module, All time slots must be configured in a channel group.

Configuration Sequence

The following Summary of Steps section provides the recommended primary configuration sequence for the Cisco RAN Service Module. These steps have configuration sub-steps or tasks within the primary steps or tasks.

Note The installation of the Cisco RAN Service Module should be completed before attempting the configuration (see the "Related Documentation" section on page ix for more information).

The configuration sequence of the Cisco RAN Service Module assumes that you will have already had some familiarity with the configuration of Cisco products. 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 products.

Note For correct CLI syntax and format, see the "Cisco RAN Service Module Command Reference" section on page A-1.

Summary of Steps

Perform the following tasks to configure the Cisco RAN Service Module.

1. Configuring the Hostname and Password, page 4-4
2. Verifying the Hostname and Password, page 4-5
3. Configuring Gigabit Ethernet Interfaces, page 4-5
4. Configuring the POS Interfaces, page 4-7
5. Configuring the Backhaul Links, page 4-9
6. Configuring GSM-Abis Links, page 4-15
7. Configuring the IOS-based Cross-connect, page 4-17
8. Configuring UMTS Links, page 4-19
9. Configuring QoS, page 4-21
10. Configuring Redundancy, page 4-29
11. Configuring for SNMP Support, page 4-30
12. Configuring Graceful Degradation, page 4-33
13. Saving Configuration Changes, page 4-34

Configuring the Hostname and Password

Two important configuration tasks that you might want to perform first are to configure the hostname and to set an encrypted password. Configuring a host name allows you to distinguish multiple Cisco routers from each other. Setting an encrypted password allows you to prevent unauthorized configuration changes.

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
```

You have entered the enable mode when the prompt changes to `Router#`.

Step 2 Enter global configuration mode.

```
Router# configure terminal

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

You have entered global configuration mode when the prompt changes to `Router(config)#`.

```
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)#
```

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

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

Step 4 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$60L4$X2JYOwoDc0.kqa1loO/w8/
.
.
.
```

Check the hostname and encrypted password, which are displayed near the top of the command output.

Step 2 Exit global configuration mode and attempt to reenter 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

The Gigabit Ethernet interfaces are numbered GigE 0/0, GigE 1/0, GigE 2/0, and GigE 3/0. Each of these interfaces is assigned to one CPU. Interface GigE 0/0 is used for management traffic. The other GigE interfaces (GigE 1/0, GigE 2/0, and GigE 3/0) are used for backhaul communications. These interfaces do not interact with other I/O cards via the cross-connect, but rather are physical RJ-45 ports available on the faceplate of the RAN Service Module.

To configure the Gigabit Ethernet (GigE) interface on the Cisco RAN Service Module, complete the following tasks:

- Configuring the Gigabit Ethernet Interface IP Address
- Setting the Speed and Duplex Mode, page 4-6
- Enabling the Gigabit Ethernet Interface, page 4-7

Configuring the Gigabit Ethernet Interface IP Address

Use the following instructions to perform a basic IP Address configuration: specifying the port adapter, assigning an IP address and subnet mask for 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 GigE interface, follow these steps, while in the global configuration mode:

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

```
Router(config)# interface gigabitethernet cpu<0-3>/port<0-0>
```

Step 2 Assign an IP address and subnet mask to the interface.

```
Router(config-if)# ip address ip_address subnet_mask
```

Setting the Speed and Duplex Mode

The Gigabit Ethernet (GigE) ports of the Cisco RAN Service Module can run in full- or half- duplex mode and at 1000 Mbps, 100 Mbps, or 10 Mbps. The Cisco RAN Service Module has an auto-negotiation feature that allows the router to negotiate the speed and duplex mode with the corresponding interface at the other end of the connection.

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

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

- If both ends of the line support auto-negotiation, we highly recommend the default auto negotiation settings.
- When auto-negotiation is turned on for either speed or duplex mode, it auto- negotiates both speed and the duplex mode.
- If one interface supports auto-negotiation, and the interface at the other end does not, configure the duplex mode and speed on both interfaces. If you use the auto-negotiation setting on the supported side, the duplex mode setting will be 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 the 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 | 10]
```

Enabling the Gigabit Ethernet 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.

Once you have configured the Gigabit Ethernet (GigE) interface, enable it, by following this step, while in the interface configuration mode:

Step 1 Enable the interface.

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

Configuring the POS Interfaces

The POS interfaces are POS 0/0, POS 1/0, POS 2/0, and POS 3/0. Each interface resides on one CPU. Interface POS 0/0 is connected to the service CPU and it may be used for management traffic. The other POS interfaces are used for backhaul communications. These interfaces support HDLC and PPP encapsulation. In CTC, the POS interfaces are listed as STM-1 ports 5-8, and they can be cross-connected to other interface cards.

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 POS interface on the Cisco RAN Service Module, complete the following tasks, while in the global configuration mode:

Step 1 Specify the port adapter type and the location of the interface to be configured. End the following command with a Ctrl/Z.

```
Router(config)# interface pos cpu<0-3>/port<0-0>
```

Step 2 Assign an IP address and subnet mask to the interface. End the following command with a Ctrl/Z.

```
Router(config-if)# ip address ip_address subnet_mask
```

Step 3 Assign the encapsulation type. End the following command with a Ctrl/Z.

```
Router(config-if)# encapsulation <encap type>
```

Step 4 Set the flag C2 byte. The default value of the C2 byte is 0x16. The C2 byte is the path signal label. The purpose of this byte is to communicate the payload type that the SONET Framing OverHead (FOH) encapsulates. The C2 byte allows a single interface to transport multiple payload types simultaneously. The C2 byte needs to be 0x16 for hdlc/ppp. End the following command with a Ctrl/Z.

```
Router(config-if)# pos flag c2 <byte value>
```

Step 5 Set the triggers for alarm generations. By default, all the following failure types trigger an alarm generation:

all - Path Signal Label Encapsulation Mismatch failure
encap - Path Signal Label Encapsulation Mismatch failure
pais - Path Alarm Indication Signal failure <default>
plmp - Path Label Mismatch failure <default>
plop - Path Loss of Pointer failure <default>
ppdi - Path Payload Defect Indication failure <default in lex encap>
prdi - Path Remote Defect Indication failure
puneq - Path Label Equivalent to Zero failure

The user can turn off any trigger by entering the **no** command in front of the trigger.

```
Router(config-if)# no pos trigger failure-types
```

Step 6 Set the trigger delay time in milli-seconds. The milli-second range is 200-2000. End the following command with a Ctrl/Z.

```
Router(config-if)# pos trigger delay milliseconds
```

Step 7 By default, POS scrambling is enabled on a Cisco RAN Service Module, and when enabled, scrambling is enabled on all POS interfaces. The command show interface pos <cpu>/<port> can be used to determine if scrambling is enabled on the RAN Service Module. The command pos-scrambling can be used to enable/disable scrambling on all POS interfaces.

Examples for this scrambling command follow:

Example 1: This command enables scrambling on all POS interfaces:

```
Router(config)# pos-scrambling
Router(config)# end
```

Example 2: This command disables scrambling on all POS interfaces:

```
Router(config)# no pos-scrambling
Router(config)# end
```

Example 3: This command shows if the state of POS scrambling:

```
Router# show interface pos cpu<0-3>/port<0-0>
Router# show interface pos 1/0
POS1/0 is down, line protocol is down
  Hardware is Packet over Sonet
  Internet address is 100.1.1.12/24
  MTU 1500 bytes, BW 155520 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive set (10 sec)
  Scramble enabled
  Last input 1d00h, output 1d00h, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   45080 packets input, 2977622 bytes
   Received 38613 broadcasts (0 IP multicast)
   0 runts, 0 giants, 0 throttles
            0 parity
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   45187 packets output, 3078744 bytes, 0 underruns
   0 output errors, 0 applique, 23 interface resets
   0 output buffer failures, 0 output buffers swapped out
   41 carrier transitions
```

Configuring the Backhaul Links

To configure the backhaul links, complete the following tasks:

- Configuring Links to E1/T1 Traffic, this page
- Configuring E1 Controllers, page 4-10
- Configuring T1 Controllers, page 4-11
- Configuring Multilink Backhaul Interface, page 4-12
- Configuring the PPP Backhaul Interfaces, page 4-14

Configuring Links to E1/T1 Traffic

There are a total of 126 E1/T1 interfaces. There are 42 of these interfaces assigned to each of the three traffic CPUs. The interface correspond to cross connect ports 9 through 134. The E1/T1interfaces serve as GSM-abis and backhaul (HDLC/PPP) connections. Users can configure up to 80 GSM-abis interfaces and 40 HDLC/PPP interfaces. No fractional E1/T1 is supported on the Cisco RAN Service Module, All time slots must be configured in a channel group.

Use the following instructions to perform a basic interface configuration: enabling the module and enabling an 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.

Step 1 Enter the enable mode.

```
Router> enable
```

Step 2 Enter the password.

```
Password: password
```

You have entered the enable mode when the prompt changes to `Router#`.

Step 3 Enter the global configuration mode.

```
Router# configure terminal
```

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

Router(config)#
```

You have entered the global configuration mode when the prompt changes to `Router(config)#`.

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.

Configuring E1 Controllers

Use the following instructions to perform a basic E1 controller configuration: specifying the E1 controller, 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 the global configuration mode:

Step 1 Specify the controller that you want to configure. Controller E1 1/0 of the Cisco RAN Service Module maps to cross connect port 9. Controller E1 1/1 maps to port 10. Or the command **show controller E1** can be used to look up the cross connect port for the controller.

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

For example, the following command configures the E1 controller on CPU 1, port 0:

```
Router(config)# controller e1 1/0
```

You have entered the controller configuration mode when the prompt changes to `Router(config-controller)#`.

Step 2 Specify the channel-group and time slots to be mapped. Once you configure a channel-group, the serial interface is automatically created.

```
Router(config-controller)# channel-group channel-no timeslots timeslot-list
```

- *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.

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

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

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

Step 3 Exit the controller configuration mode.

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

Step 4 Configure the serial interface. Specify the CPU number, port, and channel-group number.

```
Router(config)# interface serial cpu/port:channel
Router(config-if)#
```

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 5 To configure PPP encapsulation, enter the following command:

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

Step 6 Enable keepalive packets on the interface and specify the number of times keepalive packets will be sent without a response before bringing down the interface:

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

Step 7 Return to Step 1 to configure additional E1/T1 controllers.

Step 8 Exit the 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.

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

Step 2 Specify the framing type.

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

Step 3 Exit controller configuration mode.

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

Step 4 Configure the serial interface. Specify the T1 CPU number, port number, and channel-group.

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

Step 5 Enter the following command to configure PPP encapsulation.

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

Step 6 Enable keepalive packets on the interface and specify the number of times that keepalive packets will be sent without a response before the interface is brought down:

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

Step 7 Return to Step 1 to configure additional T1 controllers.

Step 8 Exit to the 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 RAN Service Module 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
- Enable Real-Time Transport Protocol (RTP) Header-Compression, page 4-13

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
```

Step 3 Enable keepalive packets on the interface and specify the number of times the keepalive packets will be 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 restricts (identifies) the multilink interface, 5, that can be negotiated:

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

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 [periodic-refresh]
```

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 CPU number, port number, and channel-group.

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

Where:

- *cpu*—CPU number.
- *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 Cpu 1, port 0, channel-group 0:

```
Router(config)# interface serial1/0:0
Router(config-if)#
```

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 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 Enable the interleaving of packets among the fragments of larger packets on the multilink ppp bundle.

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

Step 6 Specify the maximum configurable bandwidth, The default percent value is 75 percent.

```
Router(config-if)# max-reserved-bandwidth percent
```

Step 7 Specify an identification number for the multilink interface.

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

Step 8 Enable keepalive packets on the interface and specify the number of times the keepalive packets will be 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

Use the following instructions to perform a basic GSM-Abis configuration on the Cisco RAN Service Module, by entering the following Cisco IOS commands at the router prompt (see the "Understanding the Cisco RAN Service Module Interfaces" section on page 3-1 for information about slot and port numbering on the Cisco RAN Service Module). 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 the global configuration mode:

Step 1 Specify the controller that you want to configure by entering the controller configuration mode.

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

- *cpu*—CPU number.
- *port*—Number of the serial port.

```
Router(config)# controller e1 1/2
Router(config-controller)#
```

Step 2 Specify the channel-group and time slots to be mapped. Once 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 3 Exit back to global configuration mode.

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

Step 4 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 cpu/port:channel-group
```

- *cpu*—CPU number.
- *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 CPU 1, port 2, channel group 0:

```
Router(config)# interface serial 1/2:0
Router(config-if)#
```

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 5 Enter the following command to configure GSM-Abis interface encapsulation in the 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 6 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 7 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 8 Return to Step 1 to configure the additional gsm-abis links.

Step 9 Exit the interface configuration mode.

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

Configuring the IOS-based Cross-connect

The RAN Service Module is equipped with an IOS-based cross connect feature which allows multiple ATM interfaces to be assigned to a single VC4 port. This enables the provisioner to connect all three traffic CPUs to a single STM-1 interface on the RNC. There is no default configuration for this feature, so it must be configured before UMTS links can be used.

Summery of Steps:

- Assign ATM interfaces to the desired VC4 port.
- Configure the number of VPI/VCI bits assigned to each VC4 Port.
- Activate the cross-connect configuration
- Configure VC4 port cell-payload scrambling settings (optional).
- Configure sts-stream scrambling settings (optional).

Step 1 Assign ATM interfaces to the desired VC4 port.

All four ATM interfaces can be assigned to a single VC4 port, or a single interface can be assigned to each VC4 port, or some combination thereof. No ATM interface can be added to more than one VC4 port:

```
Router(config)#cross-connect vc4 port VC4 port number
```

- *VC4 port number* - The number of the VC4 port. This corresponds to STM-1 ports 1-4 shown in the card view on CTC

```
Router(config-cc)#connect interface atm number/0
```

- *Slot* - The interface number of the ATM interface. A zero corresponds to the service CPU, And numbers 1-3 correspond to traffic CPUs 1-3.

For example, to assign all ATM interfaces to VC4 port 1:

```
Router(config)#cross-connect vc4 port 1
Router(config-cc)#connect interface atm 0/0
Router(config-cc)#connect interface atm 1/0
Router(config-cc)#connect interface atm 2/0
Router(config-cc)#connect interface atm 3/0
```

Step 2 Configure the number of VPI/VCI bits assigned to each VC4 Port.

The RAN Service Module supports the configuring of PVCs out of a pool of up to 2048 PVCs. The range of values permitted for the virtual path identifier (VPI) and virtual channel identifier (VCI) portions of the PVC identifier are determined by the command:

```
Router(config-cc)#max vpi-bits number vpi bits vci-bits number vci bits
```

- *number vpi bits* - The number of bits assigned for the VPI number. Supported ranges are 0-8. A zero indicates that the VPI number is always zero.
- *number vci bits* - The number of bits assigned for the VPI number. Supported ranges are 0-11.

For example, with the following configuration of VC port 4 would permit the VPI to be configured in the range 0-7 and the VCI to be configured in the range 0-255.

```
Router(config)#cross-connect vc4 port 1
Router(config-cc)#max vpi-bits 3 vci-bits 8
```

Note The fact that the VPI/VCI bits are configured along bit boundaries introduces some limitations in the provisioning of PVCs. For example, consider that you want to assign the interface ATM0/0 to VC4 port 1 for management traffic and interfaces ATM1/0, ATM2/0, and ATM3/0, to port 2. Even if only a few PVCs are required for VC4 port 1, the pool of PVCs assignable to VC4 port 2 would be reduced to 1024. Also, note that 2048 represents the only pool from which PVCs can be selected to be configured. The actual maximum number of PVCs which can actually be simultaneously configured is 255 PVCs per UMTS peer with a maximum of 649 per traffic CPU.

Note PVCs 0/3 and 0/4 are reserved PVCs and they cannot be configured.

Step 3 Activate the cross-connect configuration.

The following configuration command causes the above configurations to be activated on the RAN Service Module. Once this command is configured, any changes made to the ATM interface assignment to VC4 ports, or any changes to the max VPI or VCI bits will require a reload of the card to take effect. Once this card is configured and stored in the startup configuration, all IOS-based cross connect commands take effect at startup time.

```
Router(config)# ran-opt atm initialize
```

Step 4 Configure sts-stream scrambling settings (optional).

By default, the RAN Service Module uses STM-1 stream scrambling. To change this, use the global configuration command ran-opt atm scrambling. This changes the stream scrambling setting for VC4 ports 1-4. For example, to disable stream scrambling use the following command:

```
Router(config)# no ran-opt atm scrambling
```

Configuring UMTS Links

Use the following instructions to perform a basic UMTS-Iub configurational on the Cisco RAN Service Module, Enter the following Cisco IOS commands at the router prompt (see the "Understanding the Cisco RAN Service Module Interfaces" section on page 3-1 for information about slot and port numbering on the Cisco RAN Service Module). 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 UMTS-Iub attributes, follow these steps while in the global configuration mode:

Step 1 Enter interface configuration mode and specify the location of the interface.

```
Router(config)# interface ATM cpu/port
```

- *cpu*—Specifies the CPU.
- *port*—Specifies the port.

For example, the following command specifies the location of the interface as ATM 1/0.

```
Router(config# interface atm1/0
```

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 Use the aggnode command to configure the interface as an aggregate node mode.

```
Router(config-if)# atm umts-iub [aggnode]
```

For example: Since the RAN-SVC module will be used as an aggregation node, use the following configuration:

```
Router(config-if)# atm umts-iub aggnode
```

Step 3 In aggregation node mode, UMTS peers are configured on subinterfaces. To select a subinterface, use the command,

```
Router(config-if)# interface ATM cpu/port.subinterface
```

For example: To configure a UMTS peer on interface ATM1/0.10:

```
Router(config-if)# interface ATM1/0.10
```

Step 4 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.

```
Router(config-subif)# umts-iub local ip-address port
```

Step 5 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 from.

```
Router(config-subif)# umts-iub remote ip-address port
```

Step 6 Create an ATM permanent virtual circuit (PVC):

```
Router(config-if)# pvc [name] vpi/vci vci [qsaal]
```

- *name*—(Optional) specifies the name of the ATM PVC interface you create.
- *vpi*—Specifies the ATM network virtual path identifier (VPI) of this PVC.
- *vci*—Specifies the ATM network virtual channel identifier (VCI) of this PVC.
- **qsaal**—(Optional) specifies the ATM adaptation layer as AAL5.

Note Typically AAL5 PVCs are defined using qsaal encapsulation. However, if the traffic profile is such that the AAL5 packets exceed normal signaling (272 bytes) payload size, it is recommended that the PVC be defined using AAL0.

This is commonly true for OAM PVCs and synchronization PVCs. NodeB Application Part (NBAP) and Access Link Control Application Part (ALCAP) PVCs can be defined using qsaal encapsulation.

For example, the following command specifies the ATM PVC interface with a VPI of 0 and a VCI of 100:

```
Router(config-if)# pvc 0/100
```

Note PVC definitions should match those on the NodeB and use the following definitions:

NBAP signaling – use qsaal
ALCAP signaling – use qsaal
AAL2 bearer – use encapsulation aal0
All other PVCs should use encapsulation aal0

Class of service should be defined to match the NodeB PVC class of service definitions. For instance, if the NodeB has defined a PVC with CBR, the PVC on the Cisco MWR 1941-DC-A router should use the same CBR definitions.

OAM can be defined on the PVCs as well. If the NodeB has OAM enabled on its PVC, OAM should be defined on the PVCs of the Cisco MWR 1941-DC-A router as well.

Step 7 Configure the ATM adaptation layer (AAL) and encapsulation type to AAL0 encapsulation.

```
Router(config-if-atm-vc)# encapsulation aal-encap
```

- *aal-encap*—Specifies the ATM adaptation layer (AAL) and encapsulation type

For example, the following command specifies the ATM adaptation layer (AAL) as AAL0:

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

Step 8 Create another ATM permanent virtual circuit (PVC):

```
Router(config-subif)# pvc [name] vpi/vci vci [qsaal]
```

- *name*—(Optional) specifies the name of the ATM PVC interface you create.
- *vpi*—Specifies the ATM network virtual path identifier (VPI) of this PVC.
- *vci*—Specifies the ATM network virtual channel identifier (VCI) of this PVC.

- **qsaal**—(Optional) specifies the ATM adaptation layer as AAL5.

For example, the following command specifies the ATM PVC interface with a VPI of 0, a VCI of 100, and a QSAAL:

```
Router(config-if)# pvc 0/200 qsaal
```

Step 9 Return to Step 1 to configure additional interfaces.

Step 10 Exit the interface configuration mode.

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

Configuring QoS

The RAN Services module supports the Low Latency Queuing (LLQ) feature. This feature feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic. The first step in configuring QOS on the RAN Services module is to classify traffic that is destined for the priority queue. The RAN Services module provides two methods for accomplishing this. First, it is possible to identify priority queue traffic by matching against the input interface. This method is cumbersome and requires adding additional match statements for each shorthaul interface. As new shorthaul interfaces are provisioned, match statements must be added to the class-map for the interfaces. The module supports a second method for identifying packets destined for the priority queue: matching against the differentiated services code point (DSCP), In this method the GSM and UMTS applications tag backhaul packets with a configured DSCP value. Because the same DSCP value can be configured for both GSM and UMTS, only a single match statement is required to classify traffic, and no changes need to be made to the class-map when new links are provisioned. The default value for both applications is express forwarding (ef).

Three new commands are added using the Interface Configuration mode for this new feature: **umts-iub set dscp**, **umts-iub set peering dscp**, and **gsm-abis set dscp** and one new ATM-VC InterfaceConfiguration command: **umts-iub set dscp** (see Appendix A, "Cisco RAN Service Module Command Reference" for detailed command information). These new commands allow you to perform the following:

- on the UMTS Shorthaul Interface
  - Set the default DSCP value with which to tag UMTS backhaul packets. Separate values can be assigned to backhaul packets containing data from the UMTS Shorthaul Interface and assigned to backhaul packets which contain peering information for the UMTS peers running on IOS.
- on the PVC of a UMTS Shorthaul Interface
  - DSCP values configured at the interface level will be applied by default to data from all PVCs. A separate DSCP may also be assigned to specific PVCs. This value supersedes the value configured at the interface level.
- on the GSM Shorthaul Interface
  - Set the DSCP value in such a way as to tag all the backhaul packets generated from the shorthaul in the GSM Abis interface.

In the following procedures, PVC 2/1 of ATM 1/0 will go to the priority queue and PVC 2/2 of ATM 1/0 will be considered the best effort traffic and will go to the Weighted Fair Queue.

Note Defining the **dscp** value under the PVC affects the way the ATM cells are bundled together as a backhaul. The more **dscp** values that are defined, the more limitations on how the ATM cells can be bundled. This, as a result, could affect backhaul efficiency. We recommend that you define at most two different **dscp** values for each shorthaul. One for llq traffic, and the other for best effort traffic.

Creating a Class Map

For each class map that you want to create, follow these steps, while in global configuration mode:

Step 1 Assign a name to your class map.

```
Router(config)# class-map [match-all | match-any] class_name
```

Where **match-any** means that a single match rule is sufficient for class membership and **match-all** means that only packets that have all the specified attributes are part of the class.

For example, the following command specifies the class map as an llq-class:

```
Router(config)# class-map match-any llq-class
```

When you enter the **class-map** command, you are in the class map configuration mode.

Step 2 To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the following command:

```
Router(config-cmap)# match ip dscp value
```

- **match ip dscp** *value* Specifies the exact value from 0 to 63 used to identify an IP DSCP value.

For example, the following command specifies cs2 to be used as a match criterion:

```
Router(config-cmap)# match ip dscp ef
```

For more information about this command, see the *Cisco IOS Quality of Service Solutions Command Reference* for your Cisco IOS Release.

Step 3 Exit the class map configuration mode.

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

Creating a Policy Map

To create a policy map, follow these steps, while in the global configuration mode:

Step 1 Assign a name to your policy map.

```
Router(config)# policy-map policy_name
```

- *policy_name*— Specifies the name of the traffic policy. The traffic policy may contain one or more traffic classes.

For example, the following command specifies the policy map of low latency queueing (LLQ).

```
Router(config)# policy-map llq-policy
```

When you enter the **policy-map** command, you are in the policy map configuration mode.

Step 2 Associate the llq-policy with a class map.

```
Router(config-pmap)# class class_name
```

- *class_name*— Specifies the name of a traffic class you want to modify.

Specify the same *class_name* as you did in Step 1in the "Creating a Class Map" section on page 4-22.

For example, the following command specifies the class as the llq-class.

```
Router(config-pmap)# class llq-class
```

When you enter the **class** command, you are in the class submode of the policy-map configuration mode.

Step 3 Allocate a percentage of bandwidth to be used for the prority queue.

```
Router(config-pmap-c)# priority percent number
```

For example, the following command specifies a **priority percent** number of 99.

```
Router(config-pmap-c)# priority percent 99
```

Step 4 Associate the llq-policy with a default class map. The default class is used for non-priority traffic.

```
Router(config-pmap-c)# class class-default
```

Step 5 Allocate the remaining bandwidth to the default class.

```
Router(config-pmap-c)# bandwitdh remaining percent number
```

For example, the following command specifies the remaining bandwidth as 1 percent.

```
Router(config-pmap-c)# bandwidth remaining percent 1
```

Step 6 Limit the queue depth of the default queue.

```
Router(config-pmap-c)# queue-limit number
```

For example, the following command limits the queue depth to 45.

```
Router(config-pmap-c)# queue-limit 45
```

Note The queue limit on the default class should be less than the hold-queue specified on the multilink interface.

Step 7 Exit the class map and policy map configuration modes.

```
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

For more information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* for your Cisco IOS Release.

Assigning GSM DSCP Values

Step 1 To assign the GSM DSCP values, first specify the serial interface that you want to configure by entering the interface configuration mode.

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

For example, the following command enables the serial interface on CPU 1, port 2, channel group 0:

```
Router(config)# interface serial 1/2:0
Router(config-if)#
```

Step 2 To set the GSM DSCP value used as the interface default DSCP value to tag the backhaul packet, use the following command:

```
Router(config-if)# gsm set dscp value
```

- *value*—A number chosen to represent that packet of traffic.

For example, the following command specifies the number 16 for the packet of traffic for the umts-iub interface:

```
Router(config-if)# gsm set dscp 46
```

Assigning UMTS DSCP Values

Step 1 Enter the interface configuration mode and specify the location of the interface.

```
Router(config)# interface atm cpu/port
```

For example, the following command specifies the location of the interface as ATM 1/0.

```
Router(config# interface atm1/0
```

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

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

Step 3 Create an ATM path on the UMTS Iub interface, enter the following command:

```
Router(config-if)# atm umts-iub
```

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

```
Router(config-if)# interface atm 1/0.1 multipoint
```

Step 5 Create an ATM permanent virtual circuit (PVC):

```
Router(config-subif)# pvc [[name][vpi/vci][vci][qsaal]]
```

- *name*—(Optional) specifies the name of the ATM PVC interface you create.
- *vpi*—Specifies the ATM network virtual path identifier (VPI) of this PVC.
- *vci*—Specifies the ATM network virtual channel identifier (VCI) of this PVC.
- **qsaal**—(Optional) specifies the ATM adaptation layer as AAL5.

Note Typically AAL5 PVCs are defined using qsaal encapsulation. However, if the traffic profile is such that the AAL5 packets exceed normal signaling (272 bytes) payload size, it is recommended that the PVC be defined using AAL0.

This is commonly true for OAM PVCs and synchronization PVCs. NodeB Application Part (NBAP) and Access Link Control Application Part (ALCAP) PVCs can be defined using qsaal encapsulation.

For example, the following command specifies the ATM PVC interface with a VPI of 2and a VCI of 1:

```
Router(config-if)# pvc 2/1
```

Note PVC definitions should match those on the NodeB and use the following definitions:

NBAP signaling – use qsaal
ALCAP signaling – use qsaal
AAL2 bearer – use encapsulation aal0
All other PVCs should use encapsulation aal0

Class of service should be defined to match the NodeB PVC class of service definitions. For instance, if the NodeB has defined a PVC with CBR, the PVC on the Cisco RAN Service Module should use the same CBR definitions.

OAM can be defined on the PVCs as well. If the NodeB has OAM enabled on its PVC, OAM should be defined on the PVCs of the Cisco RAN Service Module as well.

Step 6 Configure the ATM adaptation layer (AAL) and encapsulation type to AAL0 encapsulation.

```
Router(config-if-atm-vc)# encapsulation aal-encap
```

- *aal-encap*—Specifies the ATM adaptation layer (AAL) and encapsulation type

For example, the following command specifies the ATM adaptation layer (AAL) as AAL0:

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

Step 7 To set the DSCP value used as the interface default DSCP value to tag the backhaul packet, use the following command:

```
Router(config-if-atm-vc)# umts-iub set dscp value
```

- *value*—A number chosen to represent that packet of traffic.

For example, the following command specifies the number 16 for the packet of traffic for the umts-iub interface:

```
Router(config-if)# umts-iub set dscp 46
```

Step 8 Perform Steps 5 through 7 to set another PVC 2/2 with a umts-iub interface DSCP of 8.

Step 9 To overwrite the previous PVC 2/1 with a umts-iub interface DSCP of 16, use the following command:

```
Router(config-if)# umts-iub set dscp value
```

- *value*—A number chosen to represent that packet of traffic.

For example, the following command overwrites the number 16 for the packet of traffic for the umts-iub interface:

```
Router(config-if-atm-vc)# umts-iub set dscp 16
```

Step 10 Perform Steps 1 to 7 for ATM0/1 with a UMTS DSCP of 8.

Step 11 To overwrite the previous PVC 2/1 with a umts-iub interface DSCP of 16, use the following command:

```
Router(config-if-atm-vc)# umts-iub set dscp value
```

- *value*—A number chosen to represent that packet of traffic.

For example, the following command overwrites the number 16 for the packet of traffic for the umts-iub interface:

```
Router(config-if-atm-vc)# umts-iub set dscp 16
```

Step 12 Exit the interface configuration mode.

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

Assigning a QoS Boilerplate to an Interface

Use the following instructions to assign a QoS boilerplate to an interface: enabling a multilink interface, enable real-time packet interleaving, specifying an ID number for the multilink interface, configuring a maximum fragment size, enabling MCMP, specifying the percent of the interface bandwidth, and assigning the Qos boilerplate. 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.

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.

Step 2 Enable Transmission Control Protocol (TCP) header compression.

```
Router(config-if)# ip tcp header-compression keyword
```

For example, the following command enables IETF-Format as the header compression:

```
Router(config-if)# ip tcp header-compression ietf-format
```

Step 3 Disable the Cisco Discovery (CDP) on the interface.

```
Router(config-if)# no cdp enable
```

Step 4 By default, PFC handling is not enabled. Enter the following command to configure PFC on the router:

```
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 creates how the router handles PFC:

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

Step 5 To configure how the router handles 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, the following command allows PFC options to be accepted:

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

Step 6 By default, ACFC handling is not enabled. 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 7 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
```

Step 8 Enable multilink PPP operation.

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

Step 9 Enable real-time packet interleaving.

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

Step 10 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, 2, that can be negotiated:

```
Router(config-if)# ppp multilink group 2
```

Step 11 Enable multiclass multilink PPP (MCMP).

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

Step 12 Specify the percent of the interface bandwidth allocated for LLQ.

```
Router(config-if)# max-reserved-bandwith percent
```

- *percent*—Percent of interface bandwidth allocated for LLQ.

For example, the following command specifies the interface bandwidth allocated for LLQ as 100%:

```
Router(config-if)# max-reserved-bandwidth 100
```

Step 13 Assign the QoS boilerplate to the multilink interface.

```
Router(config-if)# service-policy output policy_name
```

- *policy_name*— LLQ.

For example, the following command assigns the QoS boilerplate to the multilink interface policy name LLQ:

```
Router(config-if)# service-policy output llq-policy
```

Step 14 Set the size of the output queue.

```
Router(config-if)# hold-queue size in | out
```

- *size*— Number of packets held in the queue.
- *in* | *out*—Direction of packets being held, either input or output.

For example, the following command sets the size of the queue for the outbound packets at 50:

```
Router(config-if)# hold-queue 50 out
```

Note Specify a **hold-queue** limit. The limit needs to be greater than the **hold-queue** depth that is defined on the default class (see the "Creating a Class Map" section on page 4-22 for more information).

Step 15 Enable Transmission Control Protocol (TCP) header compression.

```
Router(config-if)# ip tcp header-compression keyword
```

For example, the following command enables IETF-Format as the header compression:

```
Router(config-if)# ip tcp header-compression ietf-format
```

Configuring Redundancy

With the exception of the Gigabit Ethernet interface, there is no IOS configuration to be configured on the Cisco RAN Service Module. The redundancy support for the RAN Service Module is 1:N, and it is configured from CTC. The configuration on the CTC can have either one protection group with one protect card and up to seven working cards, or it can have two protection groups with one protect card and up to four working cards in each group. The revertive timer can be disabled for the Cisco RAN Service Module so a user can manually switch back during a maintenance window.

The following is a brief explanation of redundancy support for the RAN Service Module. The protect card is running and has stored copies of the configurations for each working card in its protection group. In the event of a failure on a working card, the protect card activates the corresponding configuration that it has stored. The IOS configuration on the protect card should not be modified because the protect card needs to have a clean configuration to be ready to pick up the configuration from any of the working cards in the protection group when needed. After the working card recovers, services may be reverted to the working card. After reversion occurs, the protect card resets itself to clear out the configuration and to prepare to take over in case any other card in the protection group fails.

Redundancy on the Gigabit Ethernet interface is handled as part of the same mechanism described above. There is no separate mechanism such as HSRP that needs to be configured. In the event of a failure, the standby card configures the Gigabit Ethernet interface with the same IP as the working card. However, this presents a problem in that all layer-2 adjacent devices have the layer-2 address of the working card in their ARP tables. In order to make the transition from the working card to protect card seamless, a MAC address should be configured on the Gigabit Ethernet interfaces. When the protect card activates the configuration, it will configure the MAC address of the working card. One recommendation is to configure the MAC address that is physically assigned to the Gigabit Ethernet interface. This ensures that all MAC addresses remain unique. The following example shows how to configure the physical MAC address already assigned to the interface so that it will be stored in the configuration activated by the standby card.

Step 1 Determine the physically assigned MAC address of the Gigabit Ethernet interface which is in use:

```
Router#show interfaces GigabitEthernet 0/0 | i MAC
  Hardware is BCM1255 Internal MAC, address is 0006.0052.5300 (bia 0006.0052.5300)
```

Step 2 Configure the MAC Address on the interface

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#mac-address 0006.0052.5300
```

Configuring for SNMP Support

Use the following instructions to configure for 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 RAN Service Module 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 in order 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 RAN Service Module 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:
  - **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
  - **config**—Sends configuration notifications.
  - **dspu**—Sends downstream physical unit (DSPU) notifications.
  - **entity**—Sends Entity MIB modification notifications.
  - **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
  - **frame-relay**—Sends Frame Relay notifications.
  - **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
  - **isdn**—Sends Integrated Services Digital Network (ISDN) notifications.
  - **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
  - **repeater**—Sends standard repeater (hub) notifications.
  - **rsrb**—Sends remote source-route bridging (RSRB) notifications.
  - **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
  - **rtr**—Sends SA Agent (RTR) notifications.
  - **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
  - **sdllc**—Sends SDLLC notifications.
  - **snmp**—Sends Simple Network Management Protocol (SNMP) notifications (as defined in RFC 1157).
  - **stun**—Sends serial tunnel (STUN) notifications.

- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
- **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes.
- **x25**—Sends X.25 event notifications.

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 Graceful Degradation

Congestion on the backhaul is detected 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 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 4-15).

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.

Saving Configuration Changes

After you have completed configuring your Cisco RAN Service Module, to prevent the loss of the 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 You can press **Ctrl-Z** in any mode to return immediately to enable mode (`Router#`), instead of entering **exit**, which returns you to whatever 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 RAN Service Module

You can use Cisco's network management applications, such as Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco RAN Service Module. 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
- Auto Discovery 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.

Additional information can be found in the following publications of the Cisco MWTM documentation set:

- *Cisco Mobile Wireless Transport Manager User Guide*
- *Cisco Mobile Wireless Transport Manager Release Notes*
- *Cisco Mobile Wireless Transport Manager Online Help System*

Enabling the RAN Service Module for Remote Network Management

To enable remote network management of the Cisco RAN Service Module, 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 4-5 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 for SNMP Support" section on page 4-30 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 RAN Service Module

To monitor and maintain the Cisco RAN Service Module, use the following commands:

Command	Purpose
show controllers	Displays all CPU controllers.
show controllers gigabit ethernet *cpu/port*	Displays information about initialization block, transmit ring, receive ring and errors for the Fast Ethernet controller chip.
show controllers e1	Displays information about the controller status specific to the controller hardware. It also displays statistics about the E1 link. If you specify a CPU and port number, statistics for each 15 minute period will be displayed.
show controllers t1	Displays information about the T1 controllers.
show gsm-abis efficiency [history]	Displays the history of the GSM efficiency averages for compression/decompression at 1-second, 5-second, 1-minute, 5-minute, and 1-hour intervals.
show gsm-abis errors	Displays error statistics counters of the GSM for compression/decompression.
show gsm-abis packets	Displays packet statistics counters of the GSM for compression/decompression.
show gsm-abis peering [details | brief]	Displays peering status, statistics, and history of the GSM compression/decompression.
show interface *type cpu/port:channel*	Displays the configuration and status of the specified interface.
show interface gigabit ethernet *cpu/port*	Displays the status of the Gigabit Ethernet (GigE) interface.
show ip rtp header-compression	Displays RTP header compression statistics.
show ppp multilink	Displays MLP and multilink bundle information.
show ppp multilink interface *number*	Displays multilink information for the specified interface.
show protocols	Displays the protocols configured for the router and the individual interfaces.
show umts congestion [**atm**]	Displays the UMTS Congestion state.
show umts-iub efficiency	Displays the history of the UMTS Iub interface efficiency averages for compression/decompression at 1-second, 5-second, 1-minute, 5-minute, and 1-hour intervals.

Command	Purpose
show umts-iub errors	Displays error statistics UMTS-Iub interface.
show umts-iub packets	Displays packet statistics of the UMTS-Iub interface.
show umts-iub peering [details | brief]	Displays peering status, statistics, and history of the UMTS Iub interface.
show umts-iub pvc	Displays the pvc mapping of the UMTS Iub interface
show umts-profile	Displays how the profile is defined and which interfaces are applied.
show controller vc4	Displays the status for the VC4 since some of the line information may be independent of any individual ATM interface.
show controller atm x/y	Displays the controller information for an atm controller.
show provisioned config	Displays the E1T1 controllers that have been provisioned with port configurations.

Where to Go Next

At this point you can proceed to the following:

- The Cisco IOS software configuration guide and command reference publications for more advanced configuration topics. These publications are available on the Documentation DVD that came with your router, available online at Cisco.com, or you can order printed copies.
- The *System Error Messages* and *Debug Command Reference* publications for troubleshooting information available online at Cisco.com.

APPENDIX A

Cisco RAN Service Module Command Reference

This appendix contains an alphabetical listing of new and revised commands specific to the Cisco RAN Service Router.

The following commands have been introduced:

- show umts-iub packets, page A-54
- show umts-iub peering, page A-55
- show umts-iub pvc, page A-58
- snmp-server enable traps ipran, page A-59
- snmp-server enable traps ipran alarm-gsm, page A-60
- snmp-server enable traps ipran alarm-umts, page A-61
- snmp-server enable traps ipran util, page A-62
- umts local, page A-63
- umts remote, page A-64
- umts-iub backhaul-oam, page A-65
- umts-iub backhaul-mtu, page A-66
- umts-iub backhaul-timer, page A-67
- umts-iub congestion priority, page A-68
- umts-iub congestion-control, page A-69
- umts-iub local, page A-70
- umts-iub remote, page A-71
- umts-iub set dscp, page A-72 (Interface Configuration mode)
- umts-iub set dscp, page A-73 (PVC Configuration mode)
- umts-iub set peering dscp, page A-74

The following commands were not changed but are included for your convenience:

- cdp enable, page A-5
- clear ip rtp header-compression, page A-6
- ip rtp header-compression, page A-22
- ip tcp header-compression, page A-25
- keepalive, page A-28
- load-interval, page A-30
- match ip dscp, page A-33
- show ip rtp header-compression, page A-47

atm umts-iub

To select an ATM interface for UMTS Iub traffic, use the **atm umts-iub** Interface configuration command.

atm umts-iub [aggnode]

Syntax Description

aggnode	(Optional) This keywordcauses the UMTS aplication to operate in aggregation mode, and enables multiplexing of traffic from multiple remote cell sites routers into a single outbound interface.

Command Modes Sub-Interface configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

Usage Guidelines

When configuring an interface for aggregation mode, the command is applied to the main interface level on an ATM interface. Once the interface is configured for aggregation mode, all UMTS peers must be configured at the subinterface level.

Note It is also possible to configure UMTS peering at the subinterface level for the purpose of assigning certain PVCs to an **alternative backhaul,** however, there is an important distinction between this and aggregation mode. In an **alternative backhaul** configuration, UMTS peering is configured on both the main interface and the subinterface. The alarm state of the atm interface is set by the alarm state of the UMTS peer configured on the main interface. UMTS peering is only configured at the subinterface level in aggregation mode.

Alarms on the aggregation node interface will be propagated to all remote cell site routers, however, if any remote cell site router should be in an alarm state, the alarm will not be triggered on the aggregation node atm interface. Otherwise, an alarm on a single remote site would lead to the disruption of all remote cell routers.

Examples

The following example illustrates the use of **atm umts** command.

```
Router(config)# interface ATM0/4
Router(config-if)# atm umts-iub
```

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 *number***]**

Syntax Description

type number	(Optional) Interface type and number.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(29)SM	This command was introduced.

Examples

The following example illustrates the use of the **clear gsm-abis** command.

```
Router# clear gsm-abis serial 0/0:0
```

Related Commands

Command	Description
show gsm-abis efficiency	Displays the history of GSM compression/decompression efficiency averages at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals.
show gsm-abis errors	Displays error statistics counters.
show gsm-abis packets	Displays packet statistics counters.
show gsm-abis peering [details]	Displays peering status, statistics, and history.

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

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.4(4)MR	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
cdp run	Re-enables CDP on a Cisco device.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
router odr	Enables on-demand routing on a hub router

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***]**

Syntax Description

type number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(29)SM	This command was incorporated.

Usage Guidelines

If this command is used without an interface type and number, the command clears all RTP header compression structures and statistics.

Examples

The following example clears the RTP header compression structures and statistics for multilink interface 1:

```
Router# clear ip rtp header-compression multilink1
```

Related Commands

Command	Description
ip rtp header-compression	Enables RTP header compression.

clear umts-iub

To clear the statistics displayed by the **show umts-iub** commands, use the **clear umts-iub** command in privileged EXEC mode.

clear umts-iub [atm *number***]**

Syntax Description

atm	The .
atm interface	(Optional) The interface number range is from 0 to 1.
interface number	(Optional) The serial number range is from 0/0 to 1/1.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.
12.4(9)MR	This command was modified to include atm option.

Examples

The following example illustrates the use of the **clear umts-iub** command.

```
Router# clear umts-iub atm 0/1
```

Related Commands

Command	Description
show umts-iub efficiency	Displays the history of UMTS efficiency averages at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals.
show umts-iub peer	Displays peering status, statistics, and history.

gsm-abis congestion abate

Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.

The abate detection level is defined as x milliseconds of continuous congestion abatement (that is, no congestion indications). To set the abate detection, use the **gsm-abis congestion abate** Interface configuration command.

gsm-abis congestion abate [ms]

Syntax Description

ms	Sets the number of milliseconds for the abate detection level.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how to the gsm-abis abate command is set at 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
gsm-abis congestion critical	Defines the critical timeslots that are exempt from suppression during congestion onset.
gsm-abis congestion enable	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote when congestion is detected.
gsm-abis congestion onset	Sets 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.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.

Command	Description
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.
gsm-abis remote	Configures the remote parameters for an IP/UDP backhaul connection.

gsm-abis congestion critical

Defines the critical timeslots that are exempt from suppression during congestion onset.

These are the timeslots that contain signalling and control information exchanged between the BSC and BTS. To define the critical timeslots that are exempt from suppression during congestion onset, use the **gsm-abis congestion critical** Interface configuration command.

gsm-abis congestion critical [timeslot-range]

Syntax Description

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.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how to set the timeslots 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
```

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.
gsm-abis congestion enable	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote when congestion is detected.
gsm-abis congestion onset	Sets 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.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.

Command	Description
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.
gsm-abis remote	Configures the remote parameters for an IP/UDP backhaul connection.

gsm-abis congestion enable

The congestion detection algorithm monitors the transmit jitter buffer and sends congestion indicator signals to the remote when congestion is detected. The remote will suppress all timeslots that are not defined as critical in an effort to alleviate the congestion. The goal of the congestion detection algorithm is to save the *critical* timeslots from loss of data. To enable the congestion detection algorithm, use the **gsm-abis congestion enable** Interface configuration command.

gsm-abis congestion enable

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how to enable the gsm-abis congestion:

```
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
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.
gsm-abis congestion critical	Defines the critical timeslots that are exempt from suppression during congestion onset.
gsm-abis congestion onset	Sets 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.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.

Command	Description
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.
gsm-abis remote	Configures the remote parameters for an IP/UDP backhaul connection.

gsm-abis congestion onset

Sets 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.

The onset detection level is defined as x milliseconds of continuous congestion detected. To set the congestion onset, use the **gsm-abis congestion onset** Interface configuration command.

gsm-abis congestion onset [ms]

Syntax Description

ms	Sets the number of milliseconds for the onset detection level.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

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
```

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.
gsm-abis congestion critical	Defines the critical timeslots that are exempt from suppression during congestion onset.
gsm-abis congestion enable	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote when congestion is detected.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.

Command	Description
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.
gsm-abis remote	Configures the remote parameters for an IP/UDP backhaul connection.

gsm-abis jitter

Sets the amount of transmit jitter delay for the GSM-Abis interface.If the transmit jitter is set to 4 ms, data received on the backhaul with a time equal to 0 milliseconds will be stored in the jitter buffer and transmitted with a time equal to 4 milliseconds. 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.

To set the jitter, use the **gsm-abis jitter** Interface configuration command.

gsm-abis jitter *ms*

Syntax Description

ms	Sets the number of milliseconds for the jitter. The default value is 4 ms.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

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
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.
gsm-abis congestion critical	Defines the critical timeslots that are exempt from suppression during congestion onset.
gsm-abis congestion enable	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote when congestion is detected.
gsm-abis congestion onset	Sets 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.

Command	Description
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.
gsm-abis remote	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***]**

Syntax Description

ip-address	(Optional) The IP address for the entry you wish to establish.
port	(Optional) The port you want to use for the entry you wish to establish.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how to configure the local parameters:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis local 10.10.10.2 5502
```

Related Commands

Command	Description
gsm-abis remote	Configures the remote parameters for an IP/UDP backhaul connection.

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

ip-address	(Optional) The IP address for the entry you wish to establish.
port	(Optional) The port you want to use for the entry you wish to establish.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

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
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.

gsm-abis retransmit

To enable retransmission of 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 are the use of satellite transmission facilities or multiple router hops on the backhaul network.

gsm-abis retransmit [*sample-delay***]**

Syntax Description

sample-delay	The number of duplicate samples that must be observed before the duplicate sample will be retransmitted. The *sample-delay* in a range of 5 to 255 or 100 to 5100 ms at 20 ms intervals.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how 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
```

Related Commands

Command	Description
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.
gsm-abis remote	Configures the remote parameters for an IP/UDP backhaul connection.
show gsm-abis packet	Displays packet statistics counters of the GSM compression/decompression.
show gsm-abis packet | include retransmit	Displays packet statistics counters of the GSM compression/decompression to include the repetitive sub-rate 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

value	A number from 0 to 63 that sets the GSM-Abis DSCP value.

Defaults

The default setting is **ef** for express forwarding.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

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 set dscp cs2
```

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

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.
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.

Defaults

Disabled

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

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

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0	This command was incorporated into Cisco IOS Release 12.0. This command was modified to include the **iphc-format** keyword.
12.3(2)T	This command was incorporated into Cisco IOS Release 12.3(2)T. This command was modified to include the **periodic-refresh** keyword.
12.3(4)T	This command was modified to include the **ietf-format** keyword.
12.2(25)S	This command was incorporated into Cisco IOS Release 12.2(25)S.
12.4(2)MR	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.

The 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.

The 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. Since 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.

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

Examples

The following example enables RTP header compression on the Serial1/0 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 Serial2/0 interface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip rtp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression ietf-format
Router(config-if)# ip rtp compression-connections 20
Router(config-if)# exit
```

In the following example, RTP header compression is enabled on the Serial1/0 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
clear ip rtp header-compression	Clears RTP header compression structures and statistics.
iprtp compression-connections	Specifies the total number of RTP header compression connections that can exist on an interface.
show ip rtp header-compression	Displays RTP header compression statistics.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.

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

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, all TCP packets are compressed.
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 the header compression will be used.

Defaults

Disabled

For PPP interfaces, 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
10.0	This command was introduced.
12.0	This command was incorporated. This command was modified to include the **iphc-format** keyword.
12.3(4)T	This command was incorporated. This command was modified to include the **ietf-format** keyword.
12.4(2)MR	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.

Header Compression 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 IPHC format, the default format for PPP interfaces.

Header Compression iphc-format Keyword

This command includes the **iphc-format** keyword. The **iphc-forma**t keyword indicates the type of header compression that will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, Rapid Transport 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.

Header Compression ietf-format Keyword

This command includes the **ietf-format** keyword. The **ietf-format** keyword indicates the type of header compression that will be used. For HDLC interfaces, the **ietf-format** compresses only 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 ten 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 Serial2/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified:

```
Router(config)# interface serial2/0.0
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
```

Related Commands

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

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***]**

no keepalive [*period*]

Syntax Description

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

Defaults

period: 10 seconds

If you enter only the **keepalive** command with no arguments, the default is used..

If you enter the **no keepalive** command, keepalive packets are disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)MC2	This command was incorporated.
12.2(15)MC1	This command was incorporated.
12.3(11)T	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 very useful for rapidly 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 retry parameters 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.

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-interva**l 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

seconds	Length of time for which data is used to compute load statistics. A value that is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so forth).

Defaults

300 seconds (or 5 minutes)

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.4(4)MR	This command was incorporated.

Usage Guidelines

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.

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.

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.

The **load-interval** 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 **show interface** command will be more current, and based on more instantaneous data, rather than reflecting a more average load over a longer period of time.

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.

Examples

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.

```
Router(config)# interface serial 0
Router(config-if)# load-interval 30
```

Related Commands

Command	Description
show interfaces	Displays ALC information.

max-reserved-bandwidth

To change the percent of interface bandwidth allocated for Resource Reservation Protocol (RSVP), class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PVC Interface Priority Queueing (PIPQ), use the max-reserved bandwidth command in interface configuration mode. To restore the default value, use the no form of this command.

max-reserved-bandwidth *percent*

no max-reserved-bandwidth

Syntax Description

percent	Percent of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP.

Defaults

The default percentage is 75 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command is introduced.

Usage Guidelines

The sum of all bandwidth allocation on an interface should not exceed 75 percent of the available bandwidth on an interface. The remaining 25 percent of bandwidth is used for overhead, including Layer 2 overhead, control traffic, and best-effort traffic.

If you need to allocate more than 75 percent for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ, you can use the **max-reserved-bandwidth** command. The percent argument specifies the maximum percentage of the total interface bandwidth that can be used.

If you do use the **max-reserved-bandwidth** command, make sure that not too much bandwidth is taken away from best-effort and control traffic.

Examples

In the following example, the maximum configurable bandwidth iset to 80 percent,

```
Router(config-if)# max-reserved-bandwidth 80
```

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 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 ip-dscp-value*]

Syntax Description

ip-dscp-value	Specifies the exact value from 0 to 63 used to identify an IP DSCP value.

Defaults

This command has no default behavior or values.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(9)S	This command was incorporated.
12.1(2)T	This command was incorporated.
12.4(4)MR	This command was incorporated.

Usage Guidelines

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 **match ip dscp 0 1 2 3 4 5 6 7** 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 the *ip-dscp-value* of 2 is different than a packet marked with the *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 priority50 and attach service policy priority50 to an interface. In this example, the class map called ipdscp15 will evaluate all packets entering interface Fast Ethernet 1/0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet will be 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 fa1/0/0
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.

pos-scrambling

To enable SONET payload scrambling on a POS interfaces, use the **pos-scrambling** command. To disable scrambling, use the no form of this command.

pos-scrambling

no pos-scrambling

Syntax Description

This command has no arguments or keywords.

Defaults

Scrambling is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P and 11.1 CA.	This command was added.

Usage Guidelines

SONET payload scrambling applies a self-synchronous scrambler (x^43+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density.

Both ends of the connection must use the same scrambling algorithm.

When enabling POS scrambling on a Cisco RAN Service Module, scrambling is applied on all POS interfaces. Individual POS scrambling is not allowed.

Examples

The following example enables scrambling on all POS interfaces.

```
Router(config-if)# pos scrambling
Router(config-if)# end
```

The following example disables scrambling on all POS interfaces.

```
Router(config-if)# no pos scrambling
Router(config-if)# end
```

Related Commands

Command	Description
show interface pos	Use to determine whether scrambling is enabled on the interfaces.

ppp multilink interleave

To enable interleaving of packets among the fragments of larger packets on a Multilink PPP (MLP) bundle, use the **ppp multilink interleave** command in interface configuration mode. To disable interleaving, use the no form of this command.

ppp multilink interleave

no ppp multilink interleave

SyntaxDescription This command has no arguments or keywords.

Command Modes Interface configuration

Command History

Release	Modification
11.3	This command is introduced.

Examples The following exampleshows a simple leased line interleaving configuration using a dedicated multilink interface:

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

ran-opt atm scrambling stream

To improve data reliability, randomize the ATM cell payload frames. This avoids continuous non-variable bit patterns and improves the efficiency of the ATM's cell delineation algorithms. To do this, use the **ran-opt atm scrambling stream** command in interface configuration mode. The **no** form disables scrambling.

ran-opt atm scrambling stream

Syntax Description

This command has no arguments or keywords.

Defaults

By default, payload scrambling is on for E1 links and off for T1 1inks.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(29)SM	This command was introduced.

Usage Guidelines

Normally, you do not issue the scrambling-payload command explicitly, because the default value is sufficient. On T1 links, the default B8ZS line encoding normally assures sufficient reliability. The scrambling setting must match that of the far end.

Examples

The following example shows scrambling-payload on ATM configuration:

```
Router(config)# interface ATM0/0
Router(config-if)# no ip address
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# ran-opt atm scrambling stream
```

show gsm traffic

To display 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, use the **show gsm traffic** command in privileged EXEC mode.

show gsm traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(12)MR	This command was introduced.

Examples

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

```
Router# show gsm 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)
```

show gsm-abis efficiency

To display history of the GSM compression/decompression efficiency averages at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals, 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.

show gsm-abis efficiency [history]

Syntax Description

history	Creates a graph display of the efficiency.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

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

```
Router# show gsm-abis efficiency ser0/2:0
GSM-Abis(Serial0/2:0): efficiency (1sec/5sec/1min/5min/1hr)
    compression efficiency (091/091/091/091/091%)
  decompression efficiency (091/091/091/091/091%) *estimated*

Router# sh gsm eff history ser0/2:0

mwr1   04:00:00 PM Tuesday Apr 5 2005 est


    9999999999999999999999999999999999999999999999999999999999
    1111111111111111111111111111111111111111111111111111111111
100
 90 ************************************************************
 80 ************************************************************
 70 ************************************************************
 60 ************************************************************
 50 ************************************************************
 40 ************************************************************
 30 ************************************************************
 20 ************************************************************
 10 ************************************************************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
 GSM-Abis(Serial0/2:0) compression efficiency%/sec (last 60 secs)

    999999999
    111111111
100
 90 ########*
 80 #########
 70 #########
 60 #########
 50 #########
```

```
 40 #########
 30 #########
 20 #########
 10 #########
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
 GSM-Abis(Serial0/2:0) compression efficiency%/min (last 60 mins)
   * = maximum eff%   # = average eff%



100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
 GSM-Abis(Serial0/2:0) compression efficiency%/hr (last 72 hrs)
   * = maximum eff%   # = average eff%


mwr1   04:00:03 PM Tuesday Apr 5 2005 est


    999999999999999999999999999999999999999999999999999999999
    111111111111111111111111111111111111111111111111111111111
100
 90 ************************************************************
 80 ************************************************************
 70 ************************************************************
 60 ************************************************************
 50 ************************************************************
 40 ************************************************************
 30 ************************************************************
 20 ************************************************************
 10 ************************************************************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
 GSM-Abis(Serial0/2:0) decompression efficiency%/sec (last 60 secs)

    999999999
    111111111
100
 90 ########*
 80 #########
 70 #########
 60 #########
 50 #########
 40 #########
 30 #########
 20 #########
 10 #########
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
 GSM-Abis(Serial0/2:0) decompression efficiency%/min (last 60 mins)
   * = maximum eff%   # = average eff%
```

```
100
 90
 80
 70
 60
 50
 40
 30
 20
 10
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
             0    5    0    5    0    5    0    5    0    5    0    5    0
 GSM-Abis(Serial0/2:0) decompression efficiency%/hr (last 72 hrs)
   * = maximum eff%   # = average eff%
```

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis errors

To display error statistics counters of the 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(2)MR	This command was introduced.
12.4(9)MR	The output response of this command was modified.

Examples

The following is an example of 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_txRset ================= 33
GSM-Abis(Serial0/2:0): backhaul_overun ================= 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-1 show gsm-abis errors Field Descriptions

Field	Description
tx_gsmPak_failures	Send GSM-Abis packer failed.
txPtcl_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 errCode to indentify reason.

Table A-1 show gsm-abis errors Field Descriptions (continued)

Field	Description
backhaul_rxLostPakInd	Receive backhaul_lostPak indicator
backhaul_txLostPakInd	Transmit backhaul_lostPak indicator
backhaul_missedPak	Received backhaulPak is missed/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_txPtcl_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 ipAddr.
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
clear gsm-abis	Clears the statistics displayed.

show gsm-abis packets

To display packet statistics counters of the GSM compression/decompression, use the **show gsm-abis packets** command in privileged EXEC mode. Add the **include retransmit** to see the repetitive sub-rate samples at a specific configuration level (100 ms to 5100 ms).

show gsm-abis packets

show gsm-abis packets | include retransmit

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.
12.4(9)MR	The output response for this command was modified.

Examples

The following is a **show gsm-abis packets** example of 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 is a **show gsm-abis packets | include retransmit** example of the output generated by this command.

```
Router# show gsm-abis packet | include retransmit
  rx-retransmittedCount ====== 71405
```

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis peering

To display peering status, statistics, and history of the GSM compression/decompression, use the **show gsm-abis peering** command in privileged EXEC mode.

show gsm-abis peering [details]

Syntax Description

details	Provides detail information about peering.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following are examples outputs 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 detail 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          DISCONNECTACTIVE  *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:
  Retransmition 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'

Router#show gsm-abis peering brief
Interface              Local State Local Alarm Remote Alarm Status     Protocol
Serial1/0:0            CONNECTED   clear       clear        up         up
Serial1/1:0            CONNECTED   clear       clear        up         up
Serial1/2:0            CONNECTED   clear       clear        up         up
Serial2/0:0            CONNECTED   clear       clear        up         up
Serial2/1:0            CONNECTED   clear       clear        up         up
Serial2/2:0            CONNECTED   clear       clear        up         up
Serial3/0:0            CONNECTED   clear       clear        up         up
Serial3/1:0            CONNECTED   clear       clear        up         up
Serial3/2:0            CONNECTED   clear       clear        up         up
```

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show ip rtp header-compression

To show RTP header compression statistics, use the **show ip rtp header-compression** privileged EXEC command.

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

Syntax Description

type number	(Optional) Interface type and number.
detail	(Optional) Displays details of each connection. **Note** This keyword is not supported on the Cisco MWR 1941-DC-A.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	The command output was modified to include information related to the Distributed Compressed Real-Time Transport Protocol (dCRTP) feature.
12.2(8)MC2	This command was incorporated.
12.2(15)MC1	This command was incorporated.
12.3(11)T	This command was incorporated.
12.4(2)MR	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 is sample output from the **show ip rtp header-compression** command:

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
 Interface Serial1:
  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-2 describes the significant fields shown in the display.

Table A-2 show ip rtp header-compression Field Descriptions

Field	Description
Interface Serial1	Type and number of interface.
Rcvd: total	Number of packets received on the interface.
compressed	Number of packets with compressed header.
errors	Number of errors.
dropped	Number of dropped packets.
buffer copies	Not applicable to the Cisco MWR 1941-DC-A router.
buffer failures	Not applicable to the Cisco MWR 1941-DC-A router.
Sent: total	Total number of packets sent.
compressed	Number of packets sent with compressed header.
bytes saved	Total savings in bytes as a result of compression.
bytes sent	Not applicable to the Cisco MWR 1941-DC-A 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 1941-DC-A 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 1941-DC-A router.

Related Commands

Command	Description
ip rtp compression-connections	Specifies the total number of RTP header compression connections that can exist on an interface.
ip rtp header-compression	Enables RTP header compression.

show umts traffic

To display traffic rates, in bits per second, at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals for UMTS data transmitted and received over the backhaul, use the **show umts traffic** command in privileged EXEC mode.

show umts traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(12)MR	This command was introduced.

Examples

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

```
Router# show umts traffic

UMTS-Iub(ATM1/0.1): traffic (1sec/5sec/1min/5min/1hr) units(bps)
     compression traffic(  2400/  2496/  2495/  2496/  203)
   decompression traffic( 81120/ 81120/ 80989/ 81006/ 6287)
UMTS-Iub(ATM1/0.2): traffic (1sec/5sec/1min/5min/1hr) units(bps)
     compression traffic(  0/  0/  4/  4/  1)
   decompression traffic(  0/  0/ 19/ 19/  2)
```

show umts-iub congestion

To display history of the UMTS congestion, use the **show umts-iub congestion** command in privileged EXEC mode.

show umts-iub congestion

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(4)MR1	This command is introduced.

Examples

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

```
Router# show umts congestion atm 0/1
UMTS(ATM0/1):
    Congestion: ON
    Throttled ATM cells: 415801
    Last congestion time: Dec 13 18:09.858 duration: 0h 0m 53s
```

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub efficiency

To display history of the UMTS interface efficiency averages at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals, use the **show umts-iub 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.

show umts-iub efficiency [history]

Syntax Description

history	Creates a graph display of the efficiency.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

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

```
Router# show umts eff
Router# show umts efficiency atm 0/1
UMTS(ATM0/1): efficiency (1sec/5sec/1min/5min/1hr)
   decompression efficiency (100/100/100/100/100%)
     compression efficiency (100/100/100/100/100%)
```

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub errors

To display the error statistics of the UMTS Iub interface, use the **show umts-iub errors** command in privileged EXEC mode.

show umts-iub errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following are examples of the output generated by this command.

Example 1:

Receiving traffic from shorthaul when the peering connection is not connected with the remote router yet.

```
Router# show umts errors atm 0/1
UMTS-Iub(ATM0/1): backhaul_peer_not_ready ========= 5

5 is the number of packets received from shorthaul.
```

Example 2

The peering connection is up and shorthaul is receiving traffic from a pvc that's *NOT* configured on the remote peering router's shorthaul.

```
Router# show umts errors atm 0/1
UMTS-Iub(ATM0/1):     no_remote_pvc =============== 5

5 is also the number of packets.
```

Example 3

Error statistics that the code keeps track of if the number is not zero.

```
Router# show umts errors

UMTS-Iub(ATM1/3): backhaul_peer_not_ready ===== 6
UMTS-Iub(ATM1/3): no_remote_pvc =============== 6
UMTS-Iub(ATM1/3): backhaul_invalid_pak ======== 1
UMTS-Iub(ATM1/3): decompression_failures ====== 1
UMTS-Iub(ATM1/3):     no_shorthaul_pak_available == 1
UMTS-Iub(ATM1/3): compression_failures ======== 1
UMTS-Iub(ATM1/3):     no_backhaul_pak_available === 1
UMTS-Iub(ATM1/3):     no_backhaul_interface ======= 1
UMTS-Iub(ATM1/3):     backhaul_interface_down ===== 1
```

```
UMTS-Iub(ATM1/3):     backhaul_encap_failures ===== 1
UMTS-Iub(ATM1/3):     umts_encap_failures ========= 1
UMTS-Iub(ATM1/3):     no_local_pvc ================ 1
UMTS-Iub(ATM1/3):     no_remote_pvc =============== 1
```

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub packets

To display packet statistics of the UMTS-Iub interface, use the **show umts-iub packets** command in privileged EXEC mode.

show umts-iub packets

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.
12.4(4)MR	The command output was modified to include information related to the exceeding of the Maximum Transmission Unit (MTU) of the backhaul link (see Note).

Examples

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

```
Router# show umts packets atm 0/2
UMTS-Iub(ATM0/2): packets:
  rxUMTS_count ================ 288799
  txUMTS_count ================ 288799
  rxUMTS_bytes ================ 13862352
  txUMTS_bytes ================ 13862352
  rxBackhaul_packets ========== 238484
  txBackhaul_packets ========== 247328
  rxBackhaul_bytes ============ 156844691
  txBackhaul_bytes ============ 15736957
  txBackhaul_pak_overrun ====== 0
```

Note The txBackhaul_pak_overrun line in the **show umts packets** command represents the number of times that the MTU of the backhaul link was exceeded. It does not indicate a major problem, nor does it indicate any loss of data. However, if you choose a umts backhaul-timer that is too large, then the amount of data that is available during that time period may exceed the allowed MTU of the backhaul causing 2 backhaul packets to be sent. This reduces the umts backhaul efficiency. The allowed MTU is 450 bytes for MLPPP backhauls and for other backhaul interfaces, such as FE, the allowed MTU is the physical interface MTU less the backhaul packet overhead (which is approximately 4 bytes).

show umts-iub peering

To display the peering status, statistics, and history of the UMTS Iub interface, use the **show umts-iub peering** command in privileged EXEC mode.

show umts-iub peering [details]

Syntax Description

details	Provides detail information about peering.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following are examples of the output generated by this command.

Example 1

```
Router# show umts peering atm 2/0
UMTS-Iub(ATM2/1): Peering Information
UMTS-Iub(ATM2/0 - ATM0/0):       Local (20.20.20.2:5000) States:
UMTS-Iub(ATM2/0 - ATM0/0):            Connect State: OPEN
UMTS-Iub(ATM2/0 - ATM0/0):            Congestion Control: OFF
UMTS-Iub(ATM2/0 - ATM0/0):            Version: 6
UMTS-Iub(ATM2/0 - ATM0/0):            Alarm State:
UMTS-Iub(ATM2/0 - ATM0/0):                  RX(NO ALARM)       TX(NO ALARM)
UMTS-Iub(ATM2/0 - ATM0/0):       Remote (20.20.20.3:5000) States:
UMTS-Iub(ATM2/0 - ATM0/0):            Version: 6
UMTS-Iub(ATM2/0 - ATM0/0):            Alarm State:
UMTS-Iub(ATM2/0 - ATM0/0):                  RX(NO ALARM)       TX(NO ALARM)
```

Example 2

```
Router# show umts peering detail atm 2/0
UMTS-Iub(ATM0/1): Peering Information (Version 6)
 05/15/02 02:35:50 AM: BACKHAUL UP     INIT     --> CLOSED
 05/15/02 02:35:50 AM: OPEN            CLOSED   --> CON_SENT
 05/15/02 02:35:50 AM: CLOSE           CON_SENT --> CLOSING
 05/15/02 02:35:50 AM: OPEN            CLOSING  --> STOPPING
 05/15/02 02:35:59 AM: TIMEOUT-        STOPPING --> STOPPED
 05/15/02 02:36:28 AM: OPEN            STOPPED  --> CON_SENT
 05/15/02 02:36:28 AM: RCR+            CON_SENT --> ACK_SENT
 05/15/02 02:36:28 AM: RCA             ACK_SENT --> OPEN


 03/01/02 12:00:37 AM: Local RX(NOT AVAILABLE) TX(NOT AVAILABLE),  Remote RX(NOT
AVAILABLE) TX(NOT AVAILABLE)
 05/15/02 02:35:52 AM: Local RX(NO ALARM     ) TX(NO ALARM     ),  Remote RX(NOT
AVAILABLE) TX(NOT AVAILABLE)
 05/15/02 02:36:28 AM: Local RX(NO ALARM     ) TX(NO ALARM     ),  Remote RX(NO ALARM
) TX(NO ALARM     )
```

```
Peer Info:
 No Backhaul Interface ======= 5 packets
 Backhaul Encap Failures ===== 2 packets
 RX Ctrl Paks ================ 62 packets
 RX Ctrl Bytes =============== 2078 bytes
 TX Ctrl Paks ================ 62 packets
 TX Ctrl Bytes =============== 1365 bytes
 Out Of Sequence Paks ======== 0 packets
 Backhaul QOS classify drops = 0 packets
 Version Mismatch ============ 0 packets
 Shorthaul Mismatch ========== 0 times

Peer Errors:
 No Pak Mem ================== 0 (times)
 No Event Mem ================ 0 (times)
 No VC Mem =================== 0 (times)
 No Alarm Link Mem =========== 0 (times)
 No Print Buf ================ 0 (times)
 Unknown Msg Type ============ 0 (times)
 Unexpected Attrs ============ 0 (times)
 RX Msg Length Err =========== 0 (times)
 Retransmit Counter Err ====== 0 (times)
 NULL Retransmit Err ========= 0 (times)
 PVC Delete Mismatch ========= 0 (times)
 PVC Add Existing ============ 0 (times)
```

Example 3 Brief report for all ATM interfaces

```
Router3#show umts-iub peering brief
Interface              Local State Local rx/tx  Remote rx/tx Status     Protocol
ATM1/0.1               CON_SENT    CLEAR/CLEAR  UNKWN/UNKWN  up         up
ATM2/0.1               CON_SENT    CLEAR/CLEAR  UNKWN/UNKWN  up         up
ATM2/0.2               CON_SENT    CLEAR/CLEAR  UNKWN/UNKWN  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.3(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.4               CON_SENT    CLEAR/CLEAR  UNKWN/UNKWN  up         up
ATM2/0.6(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
ATM2/0.6(ATM2/0)       OPEN        CLEAR/CLEAR  CLEAR/CLEAR  up         up
```

Example 4 with Alternate Backhaul (192.168.10.2 to 192.168.10.1)

```
Router# show umts peering
UMTS-Iub(ATM2/1): Peering Information
UMTS-Iub(ATM2/0 - ATM0/0):       Local (20.20.20.2:5000) States:
UMTS-Iub(ATM2/0 - ATM0/0):            Connect State: OPEN
UMTS-Iub(ATM2/0 - ATM0/0):            Congestion Control: OFF
UMTS-Iub(ATM2/0 - ATM0/0):            Version: 6
UMTS-Iub(ATM2/0 - ATM0/0):            Alarm State:
UMTS-Iub(ATM2/0 - ATM0/0):                  RX(NO ALARM)       TX(NO ALARM)
UMTS-Iub(ATM2/0 - ATM0/0):       Remote (20.20.20.3:5000) States:
UMTS-Iub(ATM2/0 - ATM0/0):            Version: 6
UMTS-Iub(ATM2/0 - ATM0/0):            Alarm State:
UMTS-Iub(ATM2/0 - ATM0/0):                  RX(NO ALARM)       TX(NO ALARM)

UMTS-Iub(ATM2/0 - 0/0.1): Peering Information
UMTS-Iub(ATM2/0 - 0/0.1):   Local (192.168.10.2:6666) States:
```

```
UMTS-Iub(ATM2/0 - 0/0.1):       Connect State: OPEN
UMTS-Iub(ATM2/0 - 0/0.1):       Version: 6
UMTS-Iub(ATM2/0 - 0/0.1):   Remote (192.168.10.1:6666) States:
UMTS-Iub(ATM2/0 - 0/0.1):       Version: 6
```

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub pvc

To display the pvc mapping of the UMTS Iub interface, use the **show umts-iub pvc** command in privileged EXEC mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

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

```
Router# show umts pvc
UMTS(ATM0/1): VCD info
VCD Mapping:
  Local Index(1) <--> Local VCD(1) <--> Remote Index(1)



Local VCDs (not sent):

Local VCDs (sent):
  Index(1), VPI/VCI(2/100), Encap(6), SC(0), Peak(1920), Avg/Min(0), Burst Cells(0)

Remote VCDs:
  Index(1), VPI/VCI(2/100), Encap(6), SC(0), Peak(1920), Avg/Min(0), Burst Cells(0)
```

snmp-server enable traps ipran

To enable all ipran notifications via 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 alarm-gsm notifications, use the **no** form of this command.

snmp-server enable traps ipran

no snmp-server enable traps ipran

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(2)MR1	This command was introduced.

Examples

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

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

Related Commands

Command	Description
snmp-server enable traps ipran alarm-gsm	Provides information alarms associated with GSM-Abis interfaces.
snmp-server enable traps ipran alarm-umts	Provides information alarms associated with UMTS-Iub interfaces.
snmp-server enable traps ipran util	Provides information on backhaul utilization.

snmp-server enable traps ipran alarm-gsm

To provide information alarms associated with GSM-Abis interfaces via 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

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(2)MR1	This command was introduced.

Examples

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

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

Related Commands

Command	Description
snmp-server enable traps ipran alarm-umts	Provides information alarms associated with UMTS-Iub interfaces.
snmp-server enable traps ipran util	Provides information on backhaul utilization.
snmp-server enable traps ipran	Enables all notifications.

snmp-server enable traps ipran alarm-umts

To provide information alarms associated with UMTS-Iub interfaces via Simple Network Management Protocol (SNMP) notifications (traps) available on your system, use the **snmp-server enable traps ipran alarm-umts** command in global configuration mode. To disable ipran alarm-gsm notifications, use the **no** form of this command.

snmp-server enable traps ipran alarm-umts

no snmp-server enable traps ipran alarm-umts

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(2)MR1	This command was introduced.

Examples

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

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

Related Commands

Command	Description
snmp-server enable traps ipran alarm-gsm	Provides information alarms associated with GSM-Abis interfaces.
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 via 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 alarm-gsm notifications, use the **no** form of this command.

snmp-server enable traps ipran util

no snmp-server enable traps ipran util

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(2)MR1	This command was introduced.

Examples

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

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

Related Commands

Command	Description
snmp-server enable traps ipran alarm-gsm	Provides information alarms associated with GSM-Abis interfaces.
snmp-server enable traps ipran alarm-umts	Provides information alarms associated with UMTS-Iub interfaces.
snmp-server enable traps ipran	Enables all notifications.

umts local

To configure local ip address for the atm subinterfaces, use the **umts local** Sub-Interface configuration command. This command is used when you want to off load PVC traffic from a physical ATM shorthaul to an alternate backhaul. For each alternate backhaul, you need to create a logical shorthaul by creating an atm subinterface. Traffic for the PVCs configured under this logical shorthaul will go through the corresponding alternate backhaul.

umts local [ip-address]

Syntax Description

ip-address	The IP address for the entry you wish to establish.

Command Modes

Sub-Interface configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

Examples

The following example illustrates the use of the **umts local** command in Sub-Interface command mode.

```
Router(config)# interface ATM0/4
Router(config-if)# atm umts-iub
Router(config-subif)# umts local 10.10.10.2 5504
```

Note You do not need to input udp port. The UDP port number will be inherited automatically from the base atm interface's **umts remote [ip-address] [port]** port configuration.

Related Commands

Command	Description
umts remote [**ip-address]**	This command configures remote IP address for alternate backhaul.

umts remote

To configure local ip address for the atm subinterfaces, use the **umts remote** Sub-Interface configuration command. This command is used when you want to off load one or more PVC's traffic from a physical ATM shorthaul to go over alternate backhaul. For each alternate backhaul, you need to create a logical shorthaul by creating an atm subinterface. Traffic for the PVCs configured under this logical shorthaul will go through the corresponding alternate backhaul.

umts remote [ip-address]

Syntax Description

ip-address	The IP address for the entry you wish to establish.

Command Modes

Sub-Interface configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

Examples

The following example illustrates the use **umts remote** command.

```
Router(config)# interface ATM0/4
Router(config-if)# atm umts-iub
Router(config-subif)# umts remote 10.10.10.1 5502
```

Note The port number will be inherited from the base ATM interfaces's remote port number.

Related Commands

Command	Description
umts local [**ip-address]**	This command configures the remote IP address for alternate backhaul.

umts-iub backhaul-oam

To configure the local parameters required to provide OAM cells received on the UMTS ATM interface to be sent across the backhaul, use the **umts-iub backhaul-oam** Interface configuration command. To not transport the OAM cells across the backhaul, use the **no** form of this command.

Note When using the **no** form of the command, the end devices may only use OAM loopback cells. I.610 OAM messages are not supported by the Cisco MWR 1941-DC-A router; therefore, if you are using this mode, OAM cells should be backhauled.

Additionally, the **pvc-oam manage** Interface configuration for ATM-VC commands at the PVC configuration level should be enabled for UMTS PVCs on the Cisco MWR 1941-DC-A router. These PVCs will respond to OAM cells if the no version of the **umts-iub backhaul-oam** command is used.

umts-iub backhaul-oam

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how to configure the local parameters:

```
Router(config)# interface ATM0/4
Router(config-if) atm umts-iub
Router(config-if) umts-iub local 10.10.10.2 5504
Router(config-if) umts-iub backhaul-oam
```

umts-iub backhaul-mtu

To reduce the maximum transmission unit (MTU) of the UMTS backhaul, use the **umts-iub backhaul-mtu** command.

umts-iub backhaul-mtu *byte-number*

Syntax Description

byte-number	The MTU in bytes. The range is 250 to 4440 bytes.

Defaults

The default MTU values for MLPP backhauls is 450 bytes. All other backhaul types use the MTU from the outgoing interface less 30 bytes for the UMTS backhaul header. For instance, FastEthernet backhauls would use 1500-30 = 1470 byte MTU for UMTS backhauls.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.

Examples

The following example sets the MTU value to 350 bytes:

```
Router(config)# interface ATM0/4
Router(config-if) atm umts-iub
Router(config-if) umts-iub local 10.10.10.2 5504
Router(config-if) umts-iub backhaul-mtu 350
```

umts-iub backhaul-timer

To determine how often backhaul packets are sent for UMTS, use the **umts-iub backhaul-timer** Interface configuration command. This option is commonly used for High Speed Downlink Data Packet Access (HSDPA) offload environments. HSDPA traffic requires much more bandwidth than voice/signaling traffic on UMTS. Customers can offload the HSDPA traffic to an alternate backhaul media, such as metro-Ethernet while still maintaining low latency traffic (voice/signaling) on the existing T1/E1s. By configuring a separate UMTS peer for the HSPDA interface(s) and a timer value in the 3 ms to 8 ms range, customers can reduce CPU utilization on the Cisco MWR-1941-DC-A router and save backhaul costs by sending HSDPA across the lower cost metro-Ethernet.

Note The value should be carefully selected. Typically, it should not exceed 2 ms when the backhaul is T1/E1 MLPPP. However for alternate backhaul Frame Forwarding (FF) or Gigabit Ethernet (GigE), this value can be selected at a greater value to reduce the CPU load on the platform. Depending on the load the UMTS interface and timer selected, the UMTS payload could exceed the Maximum Transmission Unit (MTU). In this case, the backhaul packets will be sent when they reach the backhaul MTU (for non-MLPPP backhauls). A maximum MTU of 450 bytes is used for MLPPP backhauls.

umts-iub backhaul-timer ? [*1-8***] timer value(in ms)**

Syntax Description

This command has no arguments or keywords.

Defaults

Timer value of 1 ms.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

Examples

The following example shows how to determine how often the backhaul packets are sent for UMTS:

```
Router(config)# interface a3/0/0
Router(config-if) umts-iub backhaul-timer ?
<1-8> timer value(in msec)
Router(config-if)#
```

umts-iub congestion priority

To configure the congestion control priority for UMTS, use the **umts-iub congestion priority** PVC configuration command.

umts-iub congestion priority [protected**] [***2-9***]**

Syntax Description

protected	The highest priority traffic which will never be throttled during congestion.
2-9	The congestion priority with 2 being the highest and 9 being the lowest priority. Lower priority traffic are throttled before higher priority traffic.

Defaults

The default setting is 9.

Command Modes

PVC configuration

Command History

Release	Modification
12.4(4)MR1	This command is introduced.

Examples

The following example shows how to configure the UMTS congestion priority:

```
Router(config-if) pvc 2/1 qsaal
Router(config-if-atm-vc) umts-iub congestion priority protected
```

Related Commands

Command	Description
umts-iub congestion-control	Enables the congestion control under the UMTS shorthaul interface.

umts-iub congestion-control

To enable control under the UMTS shorthaul interface, use the **umts-iub congestion-control** Interface configuration command.

umts-iub congestion-control

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)MR1	This command is introduced.

Examples

The following example shows how to enable congestion control under UMTS shorthaul interface:

```
Router(config-if) umts-iub congestion-control
```

Related Commands

Command	Description
umts-iub congestion control priority	Configures the congestion control priority under UMTS.

umts-iub local

To configure the local parameters required to establish an Internet Protocol/User Data Protocol (IP/UDP) backhaul connection for use with the ATM path on the UMTS Iub interface, use the **umts-iub local** Interface configuration command.

umts-iub local [**ip-address] [***port***]**

Syntax Description

ip-address	(Optional) The IP address for the entry you wish to establish.
port	(Optional) The port you want to use for the entry you wish to establish.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how to configure the local parameters:

```
Router(config)# interface ATM0/4
Router(config-if) atm umts-iub
Router(config-if) umts-iub local 10.10.10.2 5504
```

Related Commands

Command	Description
umts-iub remote	Configures the remote parameters for an IP/UDP backhaul connection.

umts-iub remote

To configure the remote parameters required to establish an Internet Protocol/User Data Protocol (IP/UDP) backhaul connection for use with the ATM path on the UMTS Iub interface, use the **umts-iub local** Interface configuration command.

umts-iub remote [**ip-address** *port*]

Syntax Description

ip-address port	(Optional) The IP address for the port and the port number you wish to establish. The port range number is 1024 to 49151.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR	This command was introduced.

Examples

The following example shows how to configure the remote parameters:

```
Router(config)# interface ATM0/4
Router(config-if) atm umts-iub
Router(config-if) umts-iub remote 10.10.10.1 5502
```

Related Commands

Command	Description
umts-iub local	Configures the local parameters for an IP/UDP backhaul connection.

umts-iub set dscp

To mark a packet by setting the differential services code point (DSCP) for UMTS-Iub value for the backhaul packet including the peering and data generated from the shorthaul, use the **umts-iub set dscp** Interface configuration command.

umts-iub set dscp *value*

Note Use this command when configuring UMTS shorthaul interfaces.

Syntax Description

value	A number from 0 to 46 that sets the UMTS-Iub DSCP value.

Defaults

The default setting is **ef** for express forwarding.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

Examples

The following example shows how to configure the parameters:

```
Router(config)# interface ATM0/4
Router(config-if) atm umts-iub
Router(config-if) umts-iub set dscp [value]
```

Related Commands

Command	Description
umts-iub set peering dscp	This command overwrites the interface default value defined in the **umts-iub set dscp** *value* and is used to tag peering backhaul packet.

umts-iub set dscp

To overwrite the interface default value defined in the **umts-iub set dscp** *value* for UMTS shorthaul interfaces and is used to tag the backhaul packet generated from traffic from a PVC, use the **umts-iub set dscp** ATM-VC configuration command.

umts-iub set dscp *value*

Note Use this command when configuring PVCs of the UMTS shorthaul interfaces

Syntax Description

value	A number from 0 to 63 that sets the UMTS-Iub DSCP value.

Defaults

The default setting is **ef** for express forwarding,

Command Modes

ATM-VC configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

Examples

The following example shows how to configure the remote parameters:

```
Router(config)# interface ATM1/0
Router(config-if)# atm umts-iub
Router(config-if)# umts-iub set dscp value
Router(config-if-atm-vc)# umts-iub set dscp value
```

Related Commands

Command	Description
umts-iub set dscp (Interface Configuration mode)	This command sets the description value used as the interface default description value to tag the backhaul packet including the peering and data generated from the shorthaul
umts-iub set peering dscp	This command overwrites the interface default value defined in the **umts-iub set dscp** *value* and is used to tag the peering backhaul packet

umts-iub set peering dscp

To overwrite the interface default value defined in the **umts-iub set dscp** *value* and is used to tag the peering backhaul packet, use the **umts-iub set peering dscp** Interface configuration command.

umts-iub set peering dscp *value*

Note Use this command when configuring UMTS shorthaul interfaces.

Syntax Description

value	A number from 0 to 63 that sets the UMTS-Iub DSCP value.

Defaults

The default setting is **ef** for express forwarding.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(4)MR	This command is introduced.

Examples

The following example shows how to configure the parameters:

```
Router(config)# interface ATM0/4
Router(config-if) atm umts-iub
Router(config-if) umts-iub set dscp value
```

Related Commands

Command	Description
umts-iub set dscp (Interface Configuration mode)	This command sets the description value used as the interface default description value to tag the backhaul packet including the peering and data generated from the shorthaul.
umts-iub set dscp (ATM-VC Configuration mode)	This command overwrites the interface default value defined in the **umts-iub set dscp** *value* for UMTS shorthaul interfaces and is used to tag the backhaul packet generated from traffic from a PVC

APPENDIX B

Configuration Examples

This appendix provides real-world examples of RAN-O configurations.

Note The network addresses in these examples are generic addresses, so you must replace them with actual addresses for you network.

Overview

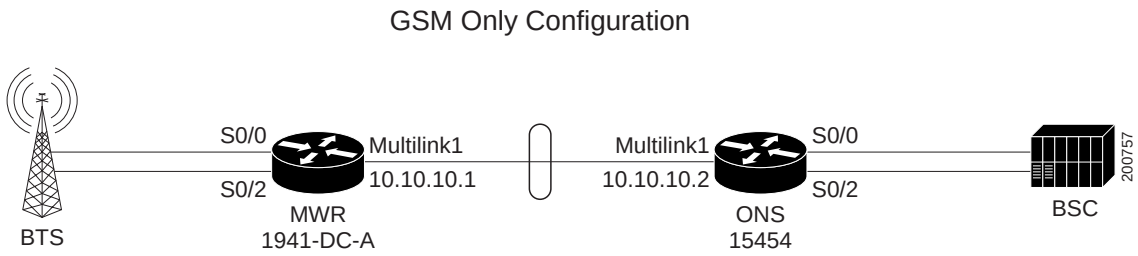
The RAN-O supports a variety of topology designs based on various GSM and UMTS configurations. Here are some common pieces to this topology:

- A *backhaul* interface is used to transfer optimized GSM/UMTS traffic between RAN-O devices. The traditional backhaul interface is comprised of one or more E1/T1 controllers logically combined to form a *multilink* connect (except HSDPA which uses the backhaul interface for E1/T1 line clocking). Future versions of RAN-O deployments will include faster backhaul interfaces (FE, GE, OC3, and so on).
- A *shorthaul* interface is used to transfer GSM and UMTS traffic from the BTS/Node-B to the Cisco MWR 1941-DC-A router to the BSC/RNC. The traditional shorthaul connections on the RAN-O devices are connected through backplane interfaces.
- Topology naming conventions such as, 3x2 and 4x3 are used to describe the type of deployment. The first number signifies the number of GSM/UMTS shorthaul interface connections while the second number signifies the number of multilink backhaul interface connections. In the case of a combined GSM/UMTS network, the conventional 3:2x2 can be used where :2 signifies the number of UMTS shorthaul interface connections.

GSM Only Configuration

The standard GSM topology includes one or more shorthaul interface connections from the BTS to a RAN-O device via separate E1/T1 connections. The RAN-O devices are connected back-to-back using a Multilink PPP backhaul connection (two or more E1/T1 connections). At the BSC side, the RAN-O to BSC connectivity is exactly like the BTS to RAN-O connections. In this scenario, only GSM traffic traverses the topology (see Figure B-1). For this example, an MWR 1941-DC-A router is to the left at the BTS side, and the Cisco RAN Service Module is housed in the Cisco ONS 15454 platform at the BSC side.

Figure B-1 GSM Only Configuration



MWR 1941-DC-A (GSM only)

```
!
card type E1 0 0
card type E1 0 1
!
!
redundancy
  mode y-cable
   standalone
!
network-clock-participate wic 0
network-clock-participate wic 1
network-clock-participate aim 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 46
 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 46
 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
```

RAN Service Module (GSM only)

```
!
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging buffered 100000 debugging
!
clock timezone PST -8
ip subnet-zero
ip cef
no ip domain-lookup
!
!
controller E1 1/0
 framing NO-CRC4
 channel-group 0 timeslots 1-31
!
controller E1 1/1
 channel-group 0 timeslots 1-31
!
controller E1 1/2
 framing NO-CRC4
 channel-group 0 timeslots 1-31
!
controller E1 1/3
!
controller E1 1/4
!
controller E1 1/5
!
controller E1 1/6
!
controller E1 1/7
!
controller E1 1/8
!
controller E1 1/9
!
controller E1 1/10
!
controller E1 1/11
!
controller E1 1/12
!
controller E1 1/13
!
controller E1 1/14
!
controller E1 1/15
!
controller E1 1/16
!
controller E1 1/17
!
controller E1 1/18
```

```
!
controller E1 1/19
!
controller E1 1/20
!
controller E1 1/21
!
controller E1 1/22
!
controller E1 1/23
!
controller E1 1/24
!
controller E1 1/25
!
controller E1 1/26
!
controller E1 1/27
!
controller E1 1/28
!
controller E1 1/29
!
controller E1 1/30
!
controller E1 1/31
!
controller E1 1/32
!
controller E1 1/33
!
controller E1 1/34
!
controller E1 1/35
!
controller E1 1/36
!
controller E1 1/37
!
controller E1 1/38
!
controller E1 1/39
!
controller E1 1/40
!
controller E1 1/41
!
controller E1 2/0
!
controller E1 2/1
!
controller E1 2/2
!
controller E1 2/3
!
controller E1 2/4
!
controller E1 2/5
!
controller E1 2/6
!
controller E1 2/7
!
controller E1 2/8
```

```
!
controller E1 2/9
!
controller E1 2/10
!
controller E1 2/11
!
controller E1 2/12
!
controller E1 2/13
!
controller E1 2/14
!
controller E1 2/15
!
controller E1 2/16
!
controller E1 2/17
!
controller E1 2/18
!
controller E1 2/19
!
controller E1 2/20
!
controller E1 2/21
!
controller E1 2/22
!
controller E1 2/23
!
controller E1 2/24
!
controller E1 2/25
!
controller E1 2/26
!
controller E1 2/27
!
controller E1 2/28
!
controller E1 2/29
!
controller E1 2/30
!
controller E1 2/31
!
controller E1 2/32
!
controller E1 2/33
!
controller E1 2/34
!
controller E1 2/35
!
controller E1 2/36
!
controller E1 2/37
!
controller E1 2/38
!
controller E1 2/39
!
controller E1 2/40
```

```
!
controller E1 2/41
!
controller E1 3/0
!
controller E1 3/1
!
controller E1 3/2
!
controller E1 3/3
!
controller E1 3/4
!
controller E1 3/5
!
controller E1 3/6
!
controller E1 3/7
!
controller E1 3/8
!
controller E1 3/9
!
controller E1 3/10
!
controller E1 3/11
!
controller E1 3/12
!
controller E1 3/13
!
controller E1 3/14
!
controller E1 3/15
!
controller E1 3/16
!
controller E1 3/17
!
controller E1 3/18
!
controller E1 3/19
!
controller E1 3/20
!
controller E1 3/21
!
controller E1 3/22
!
controller E1 3/23
!
controller E1 3/24
!
controller E1 3/25
!
controller E1 3/26
!
controller E1 3/27
!
controller E1 3/28
!
controller E1 3/29
!
controller E1 3/30
```

```
!
controller E1 3/31
!
controller E1 3/32
!
controller E1 3/33
!
controller E1 3/34
!
controller E1 3/35
!
controller E1 3/36
!
controller E1 3/37
!
controller E1 3/38
!
controller E1 3/39
!
controller E1 3/40
!
controller E1 3/41
!
!
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 10.0.0.2 255.255.255.0
 ip tcp header-compression ietf-format
 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 fragment-delay 1
 ppp multilink interleave
 ppp multilink multiclass
 multilink-group 1
 max-reserved-bandwidth 100
 service-policy output llq-policy
 hold-queue 50 out
 ip rtp header-compression ietf-format
!
interface ATM0/0
 no ip address
 loopback line
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 no negotiation auto
```

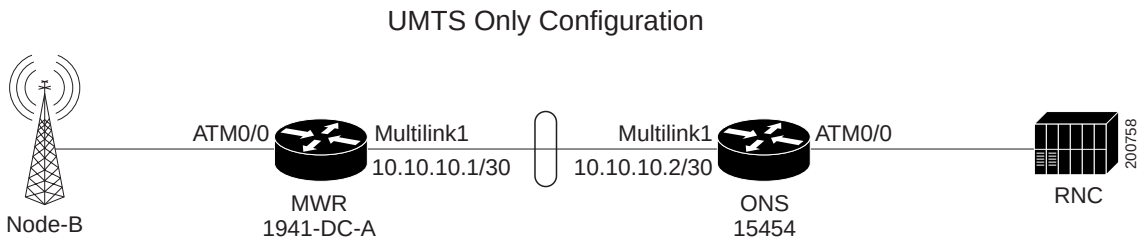
```
!
interface POS0/0
 no ip address
 loopback line

 trigger crc-error delay 0
 crc 32
!
interface ATM1/0
 no ip address
 loopback line
!
interface GigabitEthernet1/0
 no ip address
 duplex auto
 speed auto
 negotiation auto
!
interface POS1/0
 no ip address
 loopback line
 crc 32
!
interface Serial1/0:0
 no ip address
 encapsulation gsm-abis
 no keepalive
 gsm-abis local 10.0.0.2 4444
 gsm-abis remote 10.0.0.1 4444
 gsm-abis set dscp ef
!
interface Serial1/1:0
 no ip address
 encapsulation ppp
 keepalive 1
 ppp multilink
 multilink-group 1
!
interface Serial1/2:0
 no ip address
 encapsulation gsm-abis
 no keepalive
 gsm-abis local 10.0.0.2 4446
 gsm-abis remote 10.0.0.1 4446
 gsm-abis set dscp ef
!
interface ATM2/0
 no ip address
 loopback line
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
 negotiation auto
!
interface POS2/0
 no ip address
 loopback line
 crc 32
!
interface ATM3/0
 no ip address
 loopback line
```

```
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
 negotiation auto
!
interface POS3/0
 no ip address
 loopback line
 trigger crc-error threshold 0
 trigger crc-error delay 0
 crc 32
!
!
ip classless
no ip http server
!
!
tftp-server system:/memory/iosimage alias iosimage
!
!
control-plane
!
!
line con 0
 stopbits 1
line vty 0 4
 login
!
no scheduler allocate
!
```

UMTS Only Configuration

The traditional UMTS configuration is similar to the GSM configuration except only UMTS traffic traverses the topology. Unlike GSM traffic, UMTS traffic arrives at the RAN-O device via ATM PVCs. The UMTS traffic is then routed over the traditional Multilink PPP backhaul connection. At the RNC side, the RAN-O to RNC connectivity is exactly like the Node-B to RAN-O interface connections. Aside from the necessity of ATM connectivity, the physical connectivity for UMTS is exactly like the GSM topology (see Figure B-2). For this example, an MWR 1941-DC-A router is to the left at the Node-B side, and the Cisco RAN Service Module is housed in the Cisco ONS 15454 platform at the RNC side.

Figure B-2 UMTS Only Configuration



MWR 1941-DC-A (UMTS only)

```
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
card type e1 1 0
!
redundancy
  mode y-cable
   standalone
!
network-clock-participate slot 1
network-clock-participate wic 0
network-clock-participate wic 1
network-clock-participate wic 2
network-clock-participate aim 1
network-clock-select 1 E1 0/2
!
ipran-mib snmp-access inBand
ipran-mib location cellSite
!
!
controller E1 0/2
 channel-group 0 timeslots 1-31
!
controller E1 1/0
 mode atm aim 1
 clock source internal
!
class-map match-any llq-class
  match  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 4
 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 FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/2:0
 no ip address
 encapsulation ppp
 load-interval 30
 no keepalive
 ppp multilink
 ppp multilink group 1
 max-reserved-bandwidth 100
!
interface ATM1/0
 no ip address
 load-interval 30
 scrambling-payload
 no atm ilmi-keepalive
 atm umts-iub
 umts-iub congestion-control
 umts-iub backhaul-timer 1
 umts-iub set dscp ef
 umts-iub set peering dscp ef
 no umts-iub backhaul-oam
 umts-iub local 10.10.10.1 8100
 umts-iub remote 10.10.10.2 8100
 pvc 1/15
  encapsulation aal0
  umts-iub set dscp ef
  umts-iub congestion priority protected
 !
 pvc 1/112 qsaal
  umts-iub set dscp ef
 !
!
```

```
no ip http server
!
snmp-server community public RO
snmp-server ifindex persist
snmp-server trap link ietf
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 host 172.19.23.26 version 2c v2c
!
disable-eadi
```

RAN Service Module (UMTS only)

There are three separate UMTS examples shown on the following pages:

- PVC Mapping Example for UMTS, page B-13
- Profile Example for UMTS, page B-20
- VPI Mapping Example for UMTS, page B-27

PVC Mapping Example for UMTS

```
!
! Last configuration change at 18:19:50 EDT Tue Oct 24 2006
! NVRAM config last updated at 18:19:51 EDT Tue Oct 24 2006
!
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname Skyla-1
!
boot-start-marker
boot-end-marker
!
logging buffered 100000 debugging
!
!
cross-connect vc4 port 1
  connect interface atm 0/0
  max vpi-bits 1 vci-bits 6
!
!
cross-connect vc4 port 2
  connect interface atm 1/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 3
  connect interface atm 2/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 4
  connect interface atm 3/0
  max vpi-bits 1 vci-bits 8
!
```

```
ran-opt atm initialize
clock timezone EST -5
clock summer-time EDT date Apr 2 2006 2:00 Oct 29 2006 2:00
ip subnet-zero
no ip domain-lookup
!
!
ipran-mib snmp-access outOfBand
ipran-mib location aggSite
!
controller E1 1/0
!
controller E1 1/1
 channel-group 0 timeslots 1-31
!
controller E1 1/2
!
controller E1 1/3
!
controller E1 1/4
!
controller E1 1/5
!
controller E1 1/6
!
controller E1 1/7
!
controller E1 1/8
!
controller E1 1/9
!
controller E1 1/10
!
controller E1 1/11
!
controller E1 1/12
!
controller E1 1/13
!
controller E1 1/14
!
controller E1 1/15
!
controller E1 1/16
!
controller E1 1/17
!
controller E1 1/18
!
controller E1 1/19
!
controller E1 1/20
!
controller E1 1/21
!
controller E1 1/22
!
controller E1 1/23
!
controller E1 1/24
!
controller E1 1/25
!
controller E1 1/26
```

```
!
controller E1 1/27
!
controller E1 1/28
!
controller E1 1/29
!
controller E1 1/30
!
controller E1 1/31
!
controller E1 1/32
!
controller E1 1/33
!
controller E1 1/34
!
controller E1 1/35
!
controller E1 1/36
!
controller E1 1/37
!
controller E1 1/38
!
controller E1 1/39
!
controller E1 1/40
!
controller E1 1/41
!
controller E1 2/0
!
controller E1 2/1
!
controller E1 2/2
!
controller E1 2/3
!
controller E1 2/4
!
controller E1 2/5
!
controller E1 2/6
!
controller E1 2/7
!
controller E1 2/8
!
controller E1 2/9
!
controller E1 2/10
!
controller E1 2/11
!
controller E1 2/12
!
controller E1 2/13
!
controller E1 2/14
!
controller E1 2/15
!
controller E1 2/16
```

```
!
controller E1 2/17
!
controller E1 2/18
!
controller E1 2/19
!
controller E1 2/20
!
controller E1 2/21
!
controller E1 2/22
!
controller E1 2/23
!
controller E1 2/24
!
controller E1 2/25
!
controller E1 2/26
!
controller E1 2/27
!
controller E1 2/28
!
controller E1 2/29
!
controller E1 2/30
!
controller E1 2/31
!
controller E1 2/32
!
controller E1 2/33
!
controller E1 2/34
!
controller E1 2/35
!
controller E1 2/36
!
controller E1 2/37
!
controller E1 2/38
!
controller E1 2/39
!
controller E1 2/40
!
controller E1 2/41
!
controller E1 3/0
!
controller E1 3/1
!
controller E1 3/2
!
controller E1 3/3
!
controller E1 3/4
!
controller E1 3/5
!
controller E1 3/6
```

```
!
controller E1 3/7
!
controller E1 3/8
!
controller E1 3/9
!
controller E1 3/10
!
controller E1 3/11
!
controller E1 3/12
!
controller E1 3/13
!
controller E1 3/14
!
controller E1 3/15
!
controller E1 3/16
!
controller E1 3/17
!
controller E1 3/18
!
controller E1 3/19
!
controller E1 3/20
!
controller E1 3/21
!
controller E1 3/22
!
controller E1 3/23
!
controller E1 3/24
!
controller E1 3/25
!
controller E1 3/26
!
controller E1 3/27
!
controller E1 3/28
!
controller E1 3/29
!
controller E1 3/30
!
controller E1 3/31
!
controller E1 3/32
!
controller E1 3/33
!
controller E1 3/34
!
controller E1 3/35
!
controller E1 3/36
!
controller E1 3/37
!
controller E1 3/38
```

```
!
controller E1 3/39
!
controller E1 3/40
!
controller E1 3/41
!
!
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
 ip tcp header-compression ietf-format
 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 fragment-delay 0 1
 ppp multilink interleave
 ppp multilink multiclass
 multilink-group 1
 max-reserved-bandwidth 100
 service-policy output llq-policy
 hold-queue 50 out
 ip rtp header-compression ietf-format
!
interface ATM0/0
 no ip address
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface POS0/0
 no ip address
 loopback line
 crc 32
!
interface ATM1/0
 no ip address
 load-interval 30
 atm umts-iub aggnode
!
interface ATM1/0.1 multipoint
 atm umts-iub
 pvc 0/15
  encapsulation aal0
  umts-iub set dscp ef
```

```
  umts-iub congestion priority protected
  umts-iub pvc-map 1/15                    <== per pvc mapping
 !
 pvc 0/112 qsaal
  umts-iub set dscp ef
  umts-iub pvc-map 1/112                   <== per pvc mapping
 !
 umts-iub congestion-control
 umts-iub backhaul-timer 1
 umts-iub set dscp ef
 umts-iub set peering dscp ef
 umts-iub local 10.10.10.2 8100
 umts-iub remote 10.10.10.1 8100
 !
interface GigabitEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface POS1/0
 no ip address
 crc 32
!
!
interface Serial1/1:0
no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 multilink-group 1
 max-reserved-bandwidth 100
!
interface ATM2/0
 no ip address
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
!
interface POS2/0
 no ip address
 loopback line
 crc 32
!
interface ATM3/0
 no ip address
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
!
interface POS3/0
 no ip address
 crc 32
!
tftp-server system:/memory/iosimage alias iosimage
snmp-server community public RO
snmp-server ifindex persist
snmp-server trap link ietf
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
```

```
snmp-server host 172.19.23.26 version 2c v2c
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password otbu+1
 login
!
no scheduler allocate
!
```

Profile Example for UMTS

```
!
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname Skyla-1
!
boot-start-marker
boot-end-marker
!
logging buffered 100000 debugging
!
!
cross-connect vc4 port 1
  connect interface atm 0/0
  max vpi-bits 1 vci-bits 6
!
!
cross-connect vc4 port 2
  connect interface atm 1/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 3
  connect interface atm 2/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 4
  connect interface atm 3/0
  max vpi-bits 1 vci-bits 8
!
ran-opt atm initialize
clock timezone EST -5
clock summer-time EDT date Apr 2 2006 2:00 Oct 29 2006 2:00
ip subnet-zero
no ip domain-lookup
!
!
umts-profile profile_ATM1/0.1        <== define profile
 pvc cisco1 1/15
 pvc cisco2 1/112
```

```
!
ipran-mib snmp-access outOfBand
ipran-mib location aggSite
!
controller E1 1/0
!
controller E1 1/1
 channel-group 0 timeslots 1-31
!
controller E1 1/2
!
controller E1 1/3
!
controller E1 1/4
!
controller E1 1/5
!
controller E1 1/6
!
controller E1 1/7
!
controller E1 1/8
!
controller E1 1/9
!
controller E1 1/10
!
controller E1 1/11
!
controller E1 1/12
!
controller E1 1/13
!
controller E1 1/14
!
controller E1 1/15
!
controller E1 1/16
!
controller E1 1/17
!
controller E1 1/18
!
controller E1 1/19
!
controller E1 1/20
!
controller E1 1/21
!
controller E1 1/22
!
controller E1 1/23
!
controller E1 1/24
!
controller E1 1/25
!
controller E1 1/26
!
controller E1 1/27
!
controller E1 1/28
!
controller E1 1/29
```

```
!
controller E1 1/30
!
controller E1 1/31
!
controller E1 1/32
!
controller E1 1/33
!
controller E1 1/34
!
controller E1 1/35
!
controller E1 1/36
!
controller E1 1/37
!
controller E1 1/38
!
controller E1 1/39
!
controller E1 1/40
!
controller E1 1/41
!
controller E1 2/0
!
controller E1 2/1
!
controller E1 2/2
!
controller E1 2/3
!
controller E1 2/4
!
controller E1 2/5
!
controller E1 2/6
!
controller E1 2/7
!
controller E1 2/8
!
controller E1 2/9
!
controller E1 2/10
!
controller E1 2/11
!
controller E1 2/12
!
controller E1 2/13
!
controller E1 2/14
!
controller E1 2/15
!
controller E1 2/16
!
controller E1 2/17
!
controller E1 2/18
!
controller E1 2/19
```

```
!
controller E1 2/20
!
controller E1 2/21
!
controller E1 2/22
!
controller E1 2/23
!
controller E1 2/24
!
controller E1 2/25
!
controller E1 2/26
!
controller E1 2/27
!
controller E1 2/28
!
controller E1 2/29
!
controller E1 2/30
!
controller E1 2/31
!
controller E1 2/32
!
controller E1 2/33
!
controller E1 2/34
!
controller E1 2/35
!
controller E1 2/36
!
controller E1 2/37
!
controller E1 2/38
!
controller E1 2/39
!
controller E1 2/40
!
controller E1 2/41
!
controller E1 3/0
!
controller E1 3/1
!
controller E1 3/2
!
controller E1 3/3
!
controller E1 3/4
!
controller E1 3/5
!
controller E1 3/6
!
controller E1 3/7
!
controller E1 3/8
!
controller E1 3/9
```

```
!
controller E1 3/10
!
controller E1 3/11
!
controller E1 3/12
!
controller E1 3/13
!
controller E1 3/14
!
controller E1 3/15
!
controller E1 3/16
!
controller E1 3/17
!
controller E1 3/18
!
controller E1 3/19
!
controller E1 3/20
!
controller E1 3/21
!
controller E1 3/22
!
controller E1 3/23
!
controller E1 3/24
!
controller E1 3/25
!
controller E1 3/26
!
controller E1 3/27
!
controller E1 3/28
!
controller E1 3/29
!
controller E1 3/30
!
controller E1 3/31
!
controller E1 3/32
!
controller E1 3/33
!
controller E1 3/34
!
controller E1 3/35
!
controller E1 3/36
!
controller E1 3/37
!
controller E1 3/38
!
controller E1 3/39
!
controller E1 3/40
!
controller E1 3/41
```

```
!
!
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
 ip tcp header-compression ietf-format
 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 fragment-delay 0 1
 ppp multilink interleave
 ppp multilink multiclass
 multilink-group 1
 max-reserved-bandwidth 100
 service-policy output llq-policy
 hold-queue 50 out
 ip rtp header-compression ietf-format
!
interface ATM0/0
 no ip address
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface POS0/0
 no ip address
 loopback line
 crc 32
!
interface ATM1/0
 no ip address
 load-interval 30
 atm umts-iub aggnode
!
interface ATM1/0.1 multipoint
 atm umts-iub
 pvc 0/15
  encapsulation aal0
  umts-iub set dscp ef
  umts-iub congestion priority protected
  umts-iub name cisco1                    <== apply profile
  !
 pvc 0/112 qsaal
  umts-iub set dscp ef
  umts-iub name cisco2                    <== apply profile
```

```
  !
 umts-iub profile profile_ATM1/0.1 <== apply profile
 umts-iub congestion-control
 umts-iub backhaul-timer 1
 umts-iub set dscp ef
 umts-iub set peering dscp ef
 umts-iub local 10.10.10.2 8100
 umts-iub remote 10.10.10.1 8100
 !
interface GigabitEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface POS1/0
 no ip address
 crc 32
!
!
interface Serial1/1:0
no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 multilink-group 1
 max-reserved-bandwidth 100
!
interface ATM2/0
 no ip address
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
!
interface POS2/0
 no ip address
 loopback line
 crc 32
!
interface ATM3/0
 no ip address
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
!
interface POS3/0
 no ip address
 crc 32
!
tftp-server system:/memory/iosimage alias iosimage
snmp-server community public RO
snmp-server ifindex persist
snmp-server trap link ietf
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
snmp-server host 172.19.23.26 version 2c v2c
!
!
control-plane
!
```

```
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password otbu+1
 login
!
no scheduler allocate
!
```

VPI Mapping Example for UMTS

```
!
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname Skyla-1
!
boot-start-marker
boot-end-marker
!
logging buffered 100000 debugging
!
!
cross-connect vc4 port 1
  connect interface atm 0/0
  max vpi-bits 1 vci-bits 6
!
!
cross-connect vc4 port 2
  connect interface atm 1/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 3
  connect interface atm 2/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 4
  connect interface atm 3/0
  max vpi-bits 1 vci-bits 8
!
ran-opt atm initialize
clock timezone EST -5
clock summer-time EDT date Apr 2 2006 2:00 Oct 29 2006 2:00
ip subnet-zero
no ip domain-lookup
!
!
ipran-mib snmp-access outOfBand
ipran-mib location aggSite
!
controller E1 1/0
!
controller E1 1/1
 channel-group 0 timeslots 1-31
!
```

```
controller E1 1/2
!
controller E1 1/3
!
controller E1 1/4
!
controller E1 1/5
!
controller E1 1/6
!
controller E1 1/7
!
controller E1 1/8
!
controller E1 1/9
!
controller E1 1/10
!
controller E1 1/11
!
controller E1 1/12
!
controller E1 1/13
!
controller E1 1/14
!
controller E1 1/15
!
controller E1 1/16
!
controller E1 1/17
!
controller E1 1/18
!
controller E1 1/19
!
controller E1 1/20
!
controller E1 1/21
!
controller E1 1/22
!
controller E1 1/23
!
controller E1 1/24
!
controller E1 1/25
!
controller E1 1/26
!
controller E1 1/27
!
controller E1 1/28
!
controller E1 1/29
!
controller E1 1/30
!
controller E1 1/31
!
controller E1 1/32
!
controller E1 1/33
!
```

```
controller E1 1/34
!
controller E1 1/35
!
controller E1 1/36
!
controller E1 1/37
!
controller E1 1/38
!
controller E1 1/39
!
controller E1 1/40
!
controller E1 1/41
!
controller E1 2/0
!
controller E1 2/1
!
controller E1 2/2
!
controller E1 2/3
!
controller E1 2/4
!
controller E1 2/5
!
controller E1 2/6
!
controller E1 2/7
!
controller E1 2/8
!
controller E1 2/9
!
controller E1 2/10
!
controller E1 2/11
!
controller E1 2/12
!
controller E1 2/13
!
controller E1 2/14
!
controller E1 2/15
!
controller E1 2/16
!
controller E1 2/17
!
controller E1 2/18
!
controller E1 2/19
!
controller E1 2/20
!
controller E1 2/21
!
controller E1 2/22
!
controller E1 2/23
!
```

```
controller E1 2/24
!
controller E1 2/25
!
controller E1 2/26
!
controller E1 2/27
!
controller E1 2/28
!
controller E1 2/29
!
controller E1 2/30
!
controller E1 2/31
!
controller E1 2/32
!
controller E1 2/33
!
controller E1 2/34
!
controller E1 2/35
!
controller E1 2/36
!
controller E1 2/37
!
controller E1 2/38
!
controller E1 2/39
!
controller E1 2/40
!
controller E1 2/41
!
controller E1 3/0
!
controller E1 3/1
!
controller E1 3/2
!
controller E1 3/3
!
controller E1 3/4
!
controller E1 3/5
!
controller E1 3/6
!
controller E1 3/7
!
controller E1 3/8
!
controller E1 3/9
!
controller E1 3/10
!
controller E1 3/11
!
controller E1 3/12
!
controller E1 3/13
!
```

```
controller E1 3/14
!
controller E1 3/15
!
controller E1 3/16
!
controller E1 3/17
!
controller E1 3/18
!
controller E1 3/19
!
controller E1 3/20
!
controller E1 3/21
!
controller E1 3/22
!
controller E1 3/23
!
controller E1 3/24
!
controller E1 3/25
!
controller E1 3/26
!
controller E1 3/27
!
controller E1 3/28
!
controller E1 3/29
!
controller E1 3/30
!
controller E1 3/31
!
controller E1 3/32
!
controller E1 3/33
!
controller E1 3/34
!
controller E1 3/35
!
controller E1 3/36
!
controller E1 3/37
!
controller E1 3/38
!
controller E1 3/39
!
controller E1 3/40
!
controller E1 3/41
!
!
class-map match-any llq-class
  match ip dscp ef
!
!
policy-map llq-policy
  class llq-class
   priority percent 99
```

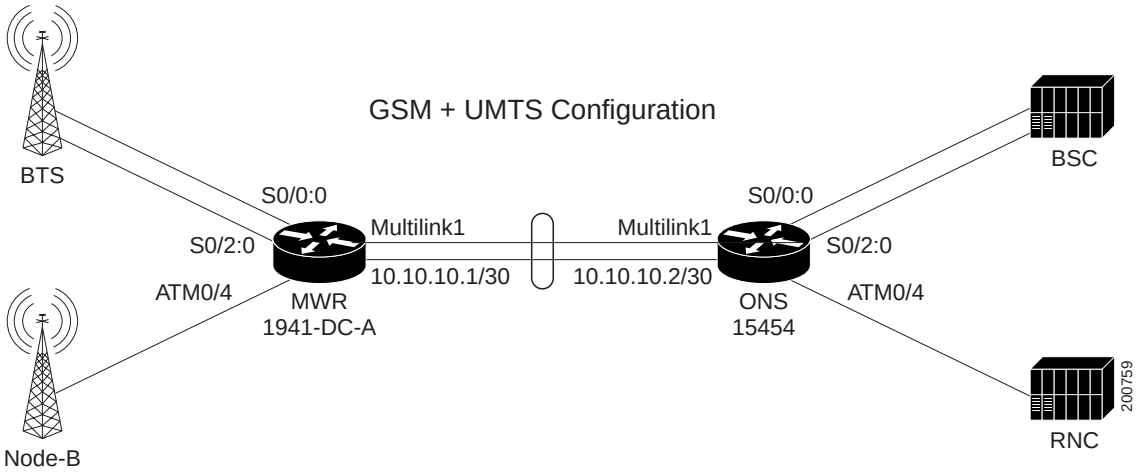
```
  class class-default
   bandwidth remaining percent 1
   queue-limit 45
!
!
!
interface Multilink1
 ip address 10.10.10.2 255.255.255.252
 ip tcp header-compression ietf-format
 load-interval 30
 no keepalive
 no cdp enable
 ppp pfc local request
 ppp pfc remote apply
 ppp acfc local request
 ppp acfc remote apply
 ppp multilink
 ppp multilink fragment-delay 0 1
 ppp multilink interleave
 ppp multilink multiclass
 multilink-group 1
 max-reserved-bandwidth 100
 service-policy output llq-policy
 hold-queue 50 out
 ip rtp header-compression ietf-format
!
interface ATM0/0
 no ip address
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface POS0/0
 no ip address
 loopback line
 crc 32
!
interface ATM1/0
 no ip address
 load-interval 30
 atm umts-iub aggnode
!
interface ATM1/0.1 multipoint
 atm umts-iub
 pvc 0/15
  encapsulation aal0
  umts-iub set dscp ef
  umts-iub congestion priority protected
  !
 pvc 0/112 qsaal
  umts-iub set dscp ef
  !
 umts-iub vpi-map 0 1                    <== vpi map
 umts-iub congestion-control
 umts-iub backhaul-timer 1
 umts-iub set dscp ef
 umts-iub set peering dscp ef
 umts-iub local 10.10.10.2 8100
 umts-iub remote 10.10.10.1 8100
 !
interface GigabitEthernet1/0
 no ip address
```

```
 duplex auto
 speed auto
!
interface POS1/0
 no ip address
 crc 32
!
interface Serial1/1:0
no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 multilink-group 1
 max-reserved-bandwidth 100
!
interface ATM2/0
 no ip address
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
!
interface POS2/0
 no ip address
 loopback line
 crc 32
!
interface ATM3/0
 no ip address
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
!
interface POS3/0
 no ip address
 crc 32
!
tftp-server system:/memory/iosimage alias iosimage
snmp-server community public RO
snmp-server ifindex persist
snmp-server trap link ietf
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
snmp-server host 172.19.23.26 version 2c v2c
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password otbu+1
 login
!
no scheduler allocate
!
```

Combined GSM and UMTS

The combined GSM and UMTS configuration allows both the GSM and UMTS technologies to become aggregated over the traditional multilink backhaul connection (see Figure B-3). For this example, an MWR 1941-DC-A router is to the left at the Node-B side, and the Cisco RAN Service Module is housed in the Cisco ONS 15454 platform at the RNC side.

Figure B-3 Combined GSM and UMTS Configuration



MWR 1941-DC-A

```
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
card type e1 1 0
!
redundancy
  mode y-cable
   standalone
!
network-clock-participate slot 1
network-clock-participate wic 0
network-clock-participate wic 1
network-clock-participate wic 2
network-clock-participate aim 1
network-clock-select 1 E1 0/2
!
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
!
controller E1 0/3
 channel-group 0 timeslots 1-31
!
controller E1 1/0
 mode atm aim 1
 clock source internal
!
class-map match-any llq-class
  match  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 4
 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 FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/0:0
 no ip address
 encapsulation gsm-abis
 gsm-abis local 10.0.0.1 4444
 gsm-abis remote 10.0.0.2 4444
 gsm-abis set dscp ef
!
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 10.0.0.1 4446
 gsm-abis remote 10.0.0.2 4446
 gsm-abis set dscp ef
!
interface Serial0/3:0
 no ip address
 encapsulation ppp
 keepalive 1
 ppp multilink group 1
 max-reserved-bandwidth 100
!
interface ATM1/0
 no ip address
 load-interval 30
 scrambling-payload
 no atm ilmi-keepalive
 atm umts-iub
 umts-iub congestion-control
 umts-iub backhaul-timer 1
 umts-iub set dscp ef
 umts-iub set peering dscp ef
 no umts-iub backhaul-oam
 umts-iub local 10.10.10.1 8100
 umts-iub remote 10.10.10.2 8100
 pvc 1/15
  encapsulation aal0
  umts-iub set dscp ef
  umts-iub congestion priority protected
 !
 pvc 1/112 qsaal
  umts-iub set dscp ef
 !
!!
!
no ip http server
!
snmp-server community public RO
snmp-server ifindex persist
snmp-server trap link ietf
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 host 172.19.23.26 version 2c v2c
!
disable-eadi
```

RAN Service Module (GSM and UMTS)

```
!
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname Skyla-1
!
boot-start-marker
boot-end-marker
!
logging buffered 100000 debugging
!
!
cross-connect vc4 port 1
  connect interface atm 0/0
  max vpi-bits 1 vci-bits 6
!
!
cross-connect vc4 port 2
  connect interface atm 1/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 3
  connect interface atm 2/0
  max vpi-bits 1 vci-bits 8
!
!
cross-connect vc4 port 4
  connect interface atm 3/0
  max vpi-bits 1 vci-bits 8
!
ran-opt atm initialize
clock timezone EST -5
clock summer-time EDT date Apr 2 2006 2:00 Oct 29 2006 2:00
ip subnet-zero
no ip domain-lookup
!
!
umts-profile profile_ATM1/0.1
 pvc cisco1 1/15
 pvc cisco2 1/112
!
ipran-mib snmp-access outOfBand
ipran-mib location aggSite
!
controller E1 1/0
 framing NO-CRC4
 channel-group 0 timeslots 1-31
!
controller E1 1/1
 channel-group 0 timeslots 1-31
!
controller E1 1/2
 framing NO-CRC4
 channel-group 0 timeslots 1-31

controller E1 1/3
 channel-group 0 timeslots 1-31
!
```

```
controller E1 1/4
!
controller E1 1/5
!
controller E1 1/6
!
controller E1 1/7
!
controller E1 1/8
!
controller E1 1/9
!
controller E1 1/10
!
controller E1 1/11
!
controller E1 1/12
!
controller E1 1/13
!
controller E1 1/14
!
controller E1 1/15
!
controller E1 1/16
!
controller E1 1/17
!
controller E1 1/18
!
controller E1 1/19
!
controller E1 1/20
!
controller E1 1/21
!
controller E1 1/22
!
controller E1 1/23
!
controller E1 1/24
!
controller E1 1/25
!
controller E1 1/26
!
controller E1 1/27
!
controller E1 1/28
!
controller E1 1/29
!
controller E1 1/30
!
controller E1 1/31
!
controller E1 1/32
!
controller E1 1/33
!
controller E1 1/34
!
controller E1 1/35
!
```

```
controller E1 1/36
!
controller E1 1/37
!
controller E1 1/38
!
controller E1 1/39
!
controller E1 1/40
!
controller E1 1/41
!
controller E1 2/0
!
controller E1 2/1
!
controller E1 2/2
!
controller E1 2/3
!
controller E1 2/4
!
controller E1 2/5
!
controller E1 2/6
!
controller E1 2/7
!
controller E1 2/8
!
controller E1 2/9
!
controller E1 2/10
!
controller E1 2/11
!
controller E1 2/12
!
controller E1 2/13
!
controller E1 2/14
!
controller E1 2/15
!
controller E1 2/16
!
controller E1 2/17
!
controller E1 2/18
!
controller E1 2/19
!
controller E1 2/20
!
controller E1 2/21
!
controller E1 2/22
!
controller E1 2/23
!
controller E1 2/24
!
controller E1 2/25
!
```

```
controller E1 2/26
!
controller E1 2/27
!
controller E1 2/28
!
controller E1 2/29
!
controller E1 2/30
!
controller E1 2/31
!
controller E1 2/32
!
controller E1 2/33
!
controller E1 2/34
!
controller E1 2/35
!
controller E1 2/36
!
controller E1 2/37
!
controller E1 2/38
!
controller E1 2/39
!
controller E1 2/40
!
controller E1 2/41
!
controller E1 3/0
!
controller E1 3/1
!
controller E1 3/2
!
controller E1 3/3
!
controller E1 3/4
!
controller E1 3/5
!
controller E1 3/6
!
controller E1 3/7
!
controller E1 3/8
!
controller E1 3/9
!
controller E1 3/10
!
controller E1 3/11
!
controller E1 3/12
!
controller E1 3/13
!
controller E1 3/14
!
controller E1 3/15
!
```

```
controller E1 3/16
!
controller E1 3/17
!
controller E1 3/18
!
controller E1 3/19
!
controller E1 3/20
!
controller E1 3/21
!
controller E1 3/22
!
controller E1 3/23
!
controller E1 3/24
!
controller E1 3/25
!
controller E1 3/26
!
controller E1 3/27
!
controller E1 3/28
!
controller E1 3/29
!
controller E1 3/30
!
controller E1 3/31
!
controller E1 3/32
!
controller E1 3/33
!
controller E1 3/34
!
controller E1 3/35
!
controller E1 3/36
!
controller E1 3/37
!
controller E1 3/38
!
controller E1 3/39
!
controller E1 3/40
!
controller E1 3/41
!
!
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
 ip tcp header-compression ietf-format
 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 fragment-delay 0 1
 ppp multilink interleave
 ppp multilink multiclass
 multilink-group 1
 max-reserved-bandwidth 100
 service-policy output llq-policy
 hold-queue 50 out
 ip rtp header-compression ietf-format
!
interface ATM0/0
 no ip address
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface POS0/0
 no ip address
 loopback line
 crc 32
!
interface ATM1/0
 no ip address
 load-interval 30
 atm umts-iub aggnode
!
interface ATM1/0.1 multipoint
 atm umts-iub
 pvc 0/15
  encapsulation aal0
  umts-iub set dscp ef
  umts-iub congestion priority protected
  umts-iub name cisco1
  !
 pvc 0/112 qsaal
  umts-iub set dscp ef
  umts-iub name cisco2
  !
 umts-iub profile profile_ATM1/0.1
 umts-iub congestion-control
 umts-iub backhaul-timer 1
 umts-iub set dscp ef
 umts-iub set peering dscp ef
 umts-iub local 10.10.10.2 8100
 umts-iub remote 10.10.10.1 8100
 !
interface GigabitEthernet1/0
 no ip address
 duplex auto
 speed auto
```

```
!
interface POS1/0
 no ip address
 crc 32
!
interface Serial1/0:0
 no ip address
 encapsulation gsm-abis
 no keepalive
 gsm-abis local 10.0.0.2 4444
 gsm-abis remote 10.0.0.1 4444
 gsm-abis set dscp ef
!
interface Serial1/1:0
 no ip address
 encapsulation ppp
 keepalive 1
 ppp multilink
 multilink-group 1
!
interface Serial1/2:0
 no ip address
 encapsulation gsm-abis
 no keepalive
 gsm-abis local 10.0.0.2 4446
 gsm-abis remote 10.0.0.1 4446
 gsm-abis set dscp ef
!
interface Serial1/3:0
no ip address
 encapsulation ppp
 load-interval 30
 ppp multilink
 multilink-group 1
 max-reserved-bandwidth 100
!
interface ATM2/0
 no ip address
!
interface GigabitEthernet2/0
 no ip address
 duplex auto
 speed auto
!
interface POS2/0
 no ip address
 loopback line
 crc 32
!
interface ATM3/0
 no ip address
!
interface GigabitEthernet3/0
 no ip address
 duplex auto
 speed auto
!
interface POS3/0
 no ip address
 crc 32
!
tftp-server system:/memory/iosimage alias iosimage
snmp-server community public RO
snmp-server ifindex persist
```

```
snmp-server trap link ietf
snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran
snmp-server host 172.19.23.26 version 2c v2c
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password otbu+1
 login
!
no scheduler allocate
!
```

C

D

E

F

G

H

I

M

P

R

S

U

V