CHAPTER 4

Configuring the Cisco 3825 Mobile Wireless Edge Router in a RAN-O Solution with the Command-Line Interface

This chapter describes how to use the Cisco IOS software CLI to configure the Cisco 3825 Mobile Wireless Edge Router in a Radio Access Network-Optimization (RAN-O) solution 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 router, return to Chapter 2 and read it now. The chapter contains important information that you need to successfully configure your router.

Before You Begin

Before you configure the Cisco 3825 router in a RAN-O solution, you should be aware of the following caveats:

- A Cisco IOS Release 12.4(16)MR1 or later, "c3825-iprank9-mz" image must be installed on the Cisco 3825 router.
- If you are using the Cisco 3825 in a redundant configuration and are attaching the router to a device that uses spanning tree, configure port first on the device to avoid problems with Hot Standby Router Protocol (HSRP) at start up.
- In case of competing equal priorities, HSRP uses the IP address to determine the active router. Therefore, you should ensure that the order of the IP addresses of the T1/E1 interfaces on the active router corresponds to the order of the IP addresses of the T1/E1 interfaces on the standby router.

Verifying the Version of Cisco IOS Software

To implement the Cisco 3825 router in a RAN-O solution, Cisco IOS Release 12.4(16)MR or later must be installed on the router. To verify the version of Cisco IOS software, use the **show version** command.

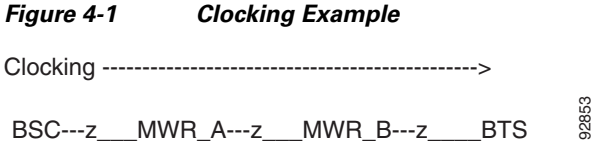
The **show version** command displays the configuration of the system hardware, the software version, the names and sources of the configuration files, and the boot images.

Clocking Requirements for Cisco 3825 Router

Network clocking is the means by which a clock signal is generated or derived and distributed through a network and its individual nodes for the purpose of ensuring synchronized network operation.

Network clocking is an important consideration in the RAN-O networks. A solid network clocking design is essential to the successful deployment of any RAN-O network. The purpose of this section is to describe the use of network clocking for RAN-O networks using the Cisco 3825 router (see Figure 4-1 for an example of clocking using the Cisco 3825 router).

Figure 4-1 Clocking Example



The Base Station Controller (BSC) is responsible for providing the clock source into the network to which the connected devices must synchronize its transmit clocks.

The BSC provides the clock source to the Cisco 3825 router, which is distributed to the participating serial/ATM ports.

Clock-Related Commands

The following sections describe the uses of the clock-related commands:

- Network-Clock-Participate Command
- Network-Clock-Select Command
- Clock Source Command

Network-Clock-Participate Command

The **network-clock-participate** command allows the ports on a specified network module or voice/WAN interface card (VWIC) or high-speed WAN interface card to use the network clock for timing. For example:

```
mwr2(config)#network-clock-participate ?

  aim   AIM  Module
  slot  Network Module Slot
  wic   WIC  Module

Use "aim" keyword to identify Advanced Integration Module
Use "wic" keyword to specify the voice/WAN interface card
```

Network-Clock-Select Command

The **network-clock-select** command names a source to provide timing for the network clock and to specify the selection priority for this clock source.

To ensure that the router uses the correct interface as the primary (highest priority) clock source, this command must be present to configure the clocking priority for the system. To establish the clocking hierarchy (in case the primary source goes down), the same command needs to be repeated with a different priority for each interface:

```
network-clock-select 1 e1 0/0/0

network-clock-select 2 e1 0/0/1
```

Clock Source Command

The **clock source** command configures the source for synchronization of the interface transmit clock.

Configure *clock source line* if the router is deriving its clock externally from the connected device.

Configure *clock source internal* if the router provides the master clock (for example, either the internal clock or the network clock).

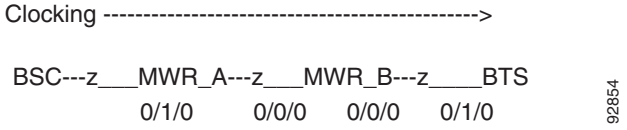
The **show network-clocks** command allows verification of the clocking configuration.

```
mwr2#sh network-clocks
  Network Clock Configuration
  ---------------------------
  Priority      Clock Source    Clock State     Clock Type

     1          E1 0/0/0      GOOD            E1
    10          Backplane       GOOD            PLL

  Current Primary Clock Source
  ---------------------------
  Priority      Clock Source    Clock State     Clock Type

     1          E1 0/0/0      GOOD            E1
```

The previous output of **show network-clocks** corresponds to the following configuration (see Figure 4-2 for description of how the clocking is done):

```
no network-clock-participate slot 1
  network-clock-participate wic 0
  network-clock-participate wic 1
  network-clock-participate wic 2
  no network-clock-participate aim 0
  no network-clock-participate aim 1
  network-clock-select 1 E1 0/0/0

  controller E1 0/0/0
   clock source line
   channel-group 0 timeslots 1-31 speed 64
```

Figure 4-2 Clocking Example



1. The BSC provides clock synchronization to the *MWR_A* router.
2. The *MWR_A* router receives clock from the BSC via port 0/1/0 and distributes to port 0/0/0.
3. The *MWR_B* router receives clock from the *MWR_A* router via port 0/0/0 and distributes to port 0/1/0.
4. The Base Transceiver STATION (BTS) receives clock synchronization from the *MWR_B* router.
5. The clock synchronization from the BSC is propagated through the network to the BTS.

Example Configurations

The following examples show two sample configurations:

Configuration Sample #1

```
  network-clock-participate wic 0
  network-clock-participate wic 1
  network-clock-select 1 E1 0/1/0

  controller E1 0/0/0
   clock source internal
   channel-group 0 timeslots 1-31 speed 64

controller E1 0/1/0
   clock source line
   channel-group 0 timeslots 1-31 speed 64
```

Configuration Sample #2

```
  network-clock-participate wic 0
  network-clock-participate wic 1
  network-clock-select 1 E1 0/0/0

  controller E1 0/0/0
   clock source line
   channel-group 0 timeslots 1-31 speed 64

controller E1 0/1/0
   clock source internal
   channel-group 0 timeslots 1-31 speed 64
```

Show Controller Command

Use the **show controller** command to detect any clocking issues. For example, *Slip Secs* may indicate a clocking issue (see following example).

```
mwr1#sh contr e1 0/1/0
E1 0/2 is up.
  Applique type is Channelized E1 - balanced
  No alarms detected.
  alarm-trigger is not set
  Version info Firmware: 20050421, FPGA: 13, spm_count = 0
  Daughter card FPGA version: 0x16, source: Bundled
  Framing is NO-CRC4, Line Code is HDB3, Clock Source is Line.
  CRC Threshold is 320. Reported from firmware  is 320.
  VWIC relays are closed
  Link noise monitor disabled
  Data in current interval (330 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     243 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
```

Note The last line of the previous example shows 243 Slip Secs indicating a possible clocking issue.

Configuration Sequence

The Summary of Steps section provides the recommended primary configuration sequence for the Cisco 3825 router in a RAN-O solution. These steps have configuration sub-steps or tasks within the primary steps or tasks.

Note The installation of the Cisco 3825 router and the Cisco 2-port T1/E1-RAN interface card should be completed before attempting the configuration (see the "Related Documentation" section on page ix for more information).

The configuration sequence of the Cisco 3825 router for the RAN-O solution assumes that you will have already had some familiarity with the configuration of Cisco routers. It is also assumed that you are familiar with your own network configurations and that you are familiar with the CLI used in configuring Cisco routers.

Note For correct CLI syntax and format, see the "Cisco 3825 Mobile Wireless Edge Router RAN-O Command Reference" section on page A-1.

Summary of Steps

Perform the following tasks to configure the Cisco 3825 router in a RAN-O solution.

1. Configuring the Hostname and Password
2. Verifying the Hostname and Password, page 4-7
3. Configuring Gigabit Ethernet Interfaces, page 4-8
4. Enabling the GE Interface, page 4-9
5. Configuring the Backhaul Links, page 4-9
6. Configuring the PPP Backhaul Interfaces, page 4-19
7. Configuring GSM-Abis Links, page 4-20
8. Configuring UMTS Links, page 4-24
9. Configuring Redundancy, page 4-28
10. Configuring for SNMP Support, page 4-33
11. Saving Configuration Changes, page 4-61

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

To configure the Gigabit Ethernet (GE) interface on the Cisco 3825 router, complete the following tasks:

- Configuring the GE Interface IP Address
- Setting the Speed and Duplex Mode, page 4-8
- Enabling the GE Interface, page 4-9

Configuring the GE Interface IP Address

Use the following instructions to perform a basic GE IP Address configuration: specifying the port adapter and aligning an IP address and subnet mask of 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 GE 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 slot/port
```

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

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 GE ports of the Cisco 3825 router can run in full- or half- duplex mode and at 1000 Mbps, 100 Mbps, or 10 Mbps. The Cisco 3825 router 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 GE Interface

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

Once you have configured the GE 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 Backhaul Links

To configure the backhaul links, complete the following tasks:

- Configuring the Card Type for the Cisco 2-port T1/E1-RAN, this page
- Configuring E1 Controllers, page 4-11
- Configuring T1 Controllers, page 4-12

Configuring the Card Type for the Cisco 2-port T1/E1-RAN

Use the following instructions to perform a basic Card Type configuration: enabling the router, enabling an interface, and specifying the card type. 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 select and configure a card type for the Cisco 2-port T1/E1-RAN card, follow these steps:

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.

Step 4 Set the card type for the Cisco 2-port T1/E1-RAN card.

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

Where:

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

For example, the following command configures the Cisco 2-port T1/E1-RAN card in the Cisco 3825 router slot 0, VWIC/HWIC slot 0 as an E1:

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

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

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

Configuring E1 Controllers

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

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

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

Step 1 Specify the controller that you want to configure. Controller E1 0/0/0 maps to the first port of the Cisco 2-port T1/E1-RAN interface card in slot 0. Controller E1 0/0/1 maps to the second port of the Cisco 2-port T1/E1-RAN interface card in slot 0.

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

For example, the following command specifies the E1 controller as the first port of the Cisco 2-port T1/E1-RAN interface card in slot 0:

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

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

Step 2 Enter the clocking source.

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

Where:

- **line**—Specifies the E1 line from which the clocking is taken.
- **internal**—Specifies internal clocking.
- **primary**—Primary clock source.

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

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

Note When you are using the **clock source {line [primary] | internal}** command to change the configuration of an installed card, you must enter the **no clock source** {**line [primary] |internal**} command first. Then enter the **clock source {line {primary] | internal}** command for the new configuration information.

Step 3 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}
```

Where:

- *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 4 Exit the controller configuration mode.

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

Step 5 Configure the serial interface. Specify the E1 slot, subslot, port number, and channel-group.

```
Router(config)# interface serial slot/subslot/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 6 To configure PPP encapsulation, enter the following command:

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

Step 7 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 [retries]]
```

Step 8 Return to Step 1 to configure the second port on the Cisco 2-port T1/E1-RAN interface card and the ports on any additional Cisco 2-port T1/E1-RAN interface cards.

Step 9 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. Controller T1 0/0/0 maps to the first port of the Cisco 2-port T1/E1-RAN interface card in slot 0. Controller T1 0/0/1 maps to the second port of the Cisco 2-port T1/E1-RAN interface card in slot 0.

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

Step 2 Specify the framing type.

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

Step 3 Specify the line code format.

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

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

Note The default speed of the channel-group is 56.

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

Step 5 Configure the cable length.

```
Router(config-controller)# cablelength feet
```

Note Although you can specify a cable length from 0 to 450 feet, the hardware recognizes only two ranges: 0 to 49 feet and 50 to 450 feet. For example, entering 35 feet uses the 0 to 49 range. If you later change the cable length to 40 feet, there is no need for reconfiguration because 40 is within the 0 to 49 range. However, if you change the cable length to 50, the 50 to 450 range must be used. The actual number that you enter is stored in the configuration file.

Step 6 Exit controller configuration mode.

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

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

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

Step 8 Enter the following command to configure PPP encapsulation.

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

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

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

Step 10 Return to Step 1 to configure the second port on the Cisco 2-port T1/E1-RAN interface card and the ports on any additional Cisco 2-port T1/E1-RAN interface cards.

Step 11 Exit to the global configuration mode.

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

Configuring Network Clocking Support

To allow the ports on the Cisco 2-port T1/E1-RAN interface card to use the network clock for timing, use the **network-clock-participate** command in the global configuration mode. To restrict the device to use only its own clock signals, use the **no** form of this command.

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 Cisco 2-port T1/E1-RAN interface card, follow these steps, while in the global configuration mode:

Step 1 Continuing with configuration of the E1, configure the network clock timing by entering:

```
Router(config)# network-clock-participate [wic | aim | slot wic-slot]
```

Where:

- **wic** *wic-slot*—Configures the Cisco 2-port T1/E1-RAN interface card slot number on the Cisco 3825 router. Valid values are 0 or 1.
- **aim**—Configures the Advanced Integration Module (AIM) for Asynchronous Transfer Mode (ATM) (AIM-ATM or AIM-ATM-8) daughter card built-in on the motherboard of the Cisco 3825 router.
- **slot**—Configures the NM-2W network interface module in the network module slot located on the Cisco 3825 router.

For example, the following command configures the Cisco 2-port T1/E1-RAN interface card to use the network clock on the 2-port T1/E1-RAN in the router chassis in slot 0:

```
Router(config)# network-clock-participate wic 0
```

Step 2 To name a source to provide timing for the network clock and to specify the selection priority for this clock source, use the **network-clock-select** command in global configuration mode. To cancel the network clock selection, use the no form of this command.

Step 3 To specify the selection priority for the clock source, enter:

```
Router(config)# network-clock-select priority {e1} slot/subslot/port
```

Where:

- *priority*—Selection priority for the clock source (1 is the highest priority). The clock with the highest priority is selected to drive the system time-division multiplexing (TDM) clocks. When the higher-priority clock source fails, the next-higher-priority clock source is selected.
- **e1**—Specifies that the slot is configured as E1.
- *slot*—Slot number identifying the controller that is the clock source.

- *subslot*—Subslot number identifying the controller that is the clock source.
- *port*—Port number identifying the controller that is the clock source.

For example, the following command specifies the clock source for E1, slot 0, subslot 0, port 0:

```
Router(config)# network-clock-select 1 e1 0/0/0
```

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 3825 router can support up to 16 E1 or T1 interfaces through the multilink interface.

Complete the following configuration tasks for a multilink backhaul interface.

- Creating a Multilink Bundle, this page
- Configuring PFC, page 4-16
- Configuring ACFC, page 4-17
- Enable Multilink and Identify the Multilink Interface, page 4-17
- Enable Real-Time Transport Protocol (RTP) Header-Compression, page 4-18

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
```

Where *group-number* is the 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]
```

Where:

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

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

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

Handling PFC and ACFC

Use the following instructions to perform Protocol Field Compression (PFC) and Address and Control Field Compression (ACFC) handling during PPP negotiation to be configured. By default, PFC/ACFC handling is not enabled.

Note The recommended PFC and ACFC handling in the Cisco 3825 router is: **acfc local request, acfc remote apply, pfc local request, and pfc remote apply**.

Configuring PFC

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

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

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

Where:

- **request**—The PFC option is included in outbound configuration requests.
- **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.

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

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

Step 2 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
```

Configuring ACFC

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

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

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

Where:

- **request**—The ACFC option is included in outbound configuration requests.
- **forbid**—The ACFC option is not sent in outbound configuration requests, and requests from a remote peer to add the ACFC option are not accepted.

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

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

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

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

Where:

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

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

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

Enable Multilink and Identify the Multilink Interface

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

Step 1 Enable multilink PPP operation.

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

Step 2 Specify an identification number for the multilink interface.

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

Where ***group-number*** is the multilink group number.

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

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

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

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

Where:

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

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

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

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

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

Step 1 Enable RTP header-compression.

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

Where:

- **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 IETF format by suppressing the IP ID in the RTP/UDP header compression:

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

Configuring the PPP Backhaul Interfaces

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

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

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

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

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

Where:

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

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

```
Router(config)# interface serial0/0/0:0
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 Specify an identification number for the multilink interface.

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

Where *group-number* is the multilink group number.

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

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

Step 6 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]
```

Where *period* is an 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
```

Extended Availability Drop and Insert (EADI)

EADI capabilities must be disabled on the Cisco 3825 router (using the **disable-eadi** global configuration command) to avoid a double-termination situation upon router reboot when the Cisco 3825 router is being used in a redundant configuration.

To disable EADI, follow these steps, while in the global configuration mode:

Step 1 Disable EADI.

```
Router(config)# disable eadi
```

Configuring GSM-Abis Links

Note The following is an example of configuring an E1 on the Cisco 2-port T1/E1-RAN interface card in a Cisco 3825 router.

Use the following instructions to perform a basic Global System for Mobile Communications (GSM)-Abis configuration on the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router, by entering the following Cisco IOS commands at the router prompt (see the "Understanding the Cisco 3825 Router Interface Numbering" section on page 3-1 for information about slot and port numbering on the Cisco 3825 router). You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

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

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

Step 1 Set the card type for the Cisco 2-port T1/E1-RAN interface card.

Note This configuration assumes that the Cisco 2-port T1/E1-RAN interface card is installed in all three Cisco 2-port T1/E1-RAN interface card slots (physical slots HWIC0, HWIC1, HWIC2, and HWIC3) of the Cisco 3825 router.

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

Where:

- **e1**—*Card type E1.*
- **t1**—*Cart type T1.*
- *slot*—Slot number of the interface.
- *subslot*—Specifies the Cisco 2-port T1/E1-RAN interface card (serial slot) port number.

For example, there is no Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC0). So, the interface card is located in physical slot HWIC1. As a result, the following command configures the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC1), first port of the Cisco 2-port T1/E1-RAN interface card as a E1:

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

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

Step 2 Specify the controller that you want to configure by entering the controller configuration mode. Controller E1 0/0/0 maps to the first port of the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC0). Controller E1 0/0/1 maps to the second port of the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC0).

Note If you install a Cisco 2-port T1/E1-RAN interface card in the Cisco 3825 router in physical slot HWIC1 (leaving physical slot HWIC0 empty), the logical interfaces in physical slot HWIC1 become Serial 0/0/0 and Serial 0/0/1. If you later add a Cisco 2-port T1/E1-RAN interface card to physical slot HWIC0, the interface numbering shifts. The configuration that you created for logical interfaces Serial 0/0/0 and Serial 0/0/1 will now be applied to the Cisco 2-port T1/E1-RAN interface card in physical slot HWIC0, and you will need to create a new configuration for the logical interfaces that you previously configured on HWIC1 (which will now be Serial 0/1/0 and Serial 0/1/1). For more information about interface numbering, see Understanding the Cisco 3825 Router Interface Numbering, page 3-1.

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

Where:

- *slot*—Number of the serial slot the 2-port T1/E1-RAN card is located in the Cisco 3825 router.
- *subslot*—Number of the serial subslot the 2-port T1/E1-RAN card is located in the Cisco 3825 router.
- *port*—Number of the serial port the 2-Port T1/E1-RAN card is using.

With a Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router slot 0 (physical slot HWIC0), for example, the following command specifies the E1 controller as the first port of the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router slot 0 (physical slot HWIC0):

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

Step 3 Enter the clocking source (see Clocking Requirements for Cisco 3825 Router, page 4-2 for more information).

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

Where:

- **line**—Specifies the E1 line from which the clocking is taken.
- **internal**—Specifies internal clocking.
- **primary**—Primary clock source.

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

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

Note When you are using the **clock source {line [primary] | internal}** command to change the configuration of an installed card, you must enter the **no clock source** {**line [primary] |internal**} command first. Then enter the **clock source {line {primary] | internal}** command for the new configuration information.

Step 4 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}
```

Where:

- *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 5 Exit back to global configuration mode.

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

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

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

Where:

- *slot*—Number of the slot being configured.
- *subslot*—Number of the subslot being configured.

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

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

```
Router(config)# interface serial 0/1/0:0
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 7 Enter the following command to configure GSM-Abis interface encapsulation in the interface configuration mode.

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

Where **gsm-abis** is the type of interface layer.

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

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

Step 8 To configure the local parameters required to establish an Internet Protocol/User Datagram Protocol (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
```

Where:

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

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

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

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

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

Where:

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

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

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

Step 10 Return to Step 1 to configure the next port of the Cisco 2-port T1/E1-RAN interface card and any other ports on additional Cisco 2-port T1/E1-RAN interface cards.

Step 11 Exit the interface configuration mode.

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

Configuring UMTS Links

Note The following is an example of configuring an E1 on the Cisco 2-port T1/E1-RAN interface card in a Cisco 3825 router.

Use the following instructions to perform a basic Universal Mobile Telecommunications System (UMTS)-Iub configurational on the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router, enter the following Cisco IOS commands at the router prompt (see the "Understanding the Cisco 3825 Router Interface Numbering" section on page 3-1 for information about slot and port numbering on the Cisco 3825 router). You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

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

To configure the UMTS-Iub attributes, follow these steps beginning in the global configuration mode:

Step 1 Set the card type for the Cisco 2-port T1/E1-RAN interface card.

Note This configuration assumes that the Cisco 2-port T1/E1-RAN interface card is installed in all three Cisco 2-port T1/E1-RAN interface card slots (physical slots HWIC0, HWIC1, HWIC2, and HWIC3) of the Cisco 3825 router.

- ***e1***—*Card type E1.*
- ***t1***—*Cart type T1.*
- *slot*—Slot number of the interface.
- *subslot*—Specifies the Cisco 2-port T1/E1-RAN interface card (serial slot) port number.

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

For example, there is no Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC0). So, the interface card is located in physical slot HWIC1. As a result, the following command configures the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC1), the first port of the Cisco 2-port T1/E1-RAN interface card as a E1:

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

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

Step 2 Specify the controller that you want to configure by entering the controller configuration mode. Controller E1 0/0/0 maps to the first port of the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC0). Controller E1 0/0/1 maps to the second port of the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC0).

Note If you install a Cisco 2-port T1/E1-RAN interface card in the Cisco 3825 router in physical slot HWIC1 (leaving physical slot HWIC0 empty), the logical interfaces in physical slot HWIC1 become Serial 0/0/0 and Serial 0/0/1. If you later add a Cisco 2-port T1/E1-RAN interface card to physical slot HWIC0, the logical interface numbering shifts. The configuration that you created for interfaces Serial 0/0/0 and Serial 0/0/1 will now be applied to the Cisco 2-port T1/E1-RAN interface card in physical slot HWIC0, and you will need to create a new configuration for the logical interfaces that you previously configured on HWIC1 (which will now be Serial 0/1/0 and Serial 0/1/1). For more information about interface numbering, see Understanding the Cisco 3825 Router Interface Numbering, page 3-1.

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

Where:

- *slot*—Number of serial slot the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router.
- *subslot*—Number of serial subslot the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router.
- *port*—Number of the serial port the Cisco 2-Port T1/E1-RAN interface card is using.

With a Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router slot 0 (physical slot HWIC0), for example, the following command specifies the E1 controller as the first port of the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router serial slot 0 (physical slot HWIC0):

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

Step 3 Configure the AIM for ATM card to be used for ATM traffic on the previously specified E1 controller.

```
Router(config-controller)# mode atm aim aim-slot
```

Where *aim-slot* sets the mode of the E1 controller in the AIM slot.

For example, the following command sets the mode of the E1 controller in AIM slot 1:

```
Router(config-controller)# mode atm aim 1
```

Step 4 Enter the clocking source.

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

Where:

- **line**—Specifies the E1 line from which the clocking is taken.
- **internal**—Specifies internal clocking.
- **primary**—Primary clock source.

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

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

Note When you are using the **clock source {line [primary] | internal}** command to change the configuration of an installed card, you must enter the **no clock source** {**line [primary] |internal**} command first. Then enter the **clock source {line {primary] | internal}** command for the new configuration information.

Step 5 Exit the controller configuration mode.

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

Step 6 Configure the network clock support for the Cisco 2-port T1/E1-RAN interface card.

```
Router(config)# network-clock-participate wic number
```

Where *number* is the slot number of the Cisco 2-port T1/E1-RAN interface card which is installed on the Cisco 3825 router.

For example, the following command enables the Cisco 2-port T1/E1-RAN interface card in logical slot 2 (physical slot HWIC1) of the Cisco 3825 router to use the network clock for its timing:

```
Router(config)# network-clock-participate wic 1
```

Step 7 Configure the network clock support for the AIM for ATM card interface.

```
Router(config)# network-clock-participate aim number
```

Where *number* is the slot number of the AIM for ATM card interface installed in the Cisco 3825 router.

For example, the following command enables the AIM for ATM card interface in physical slot 1 of the Cisco 3825 router to use the network clock for its timing:

```
Router(config)# network-clock-participate aim 1
```

Step 8 To configure the UMTS-Iub interface, first specify the ATM interface by entering the interface configuration mode.

```
Router(config)# interface ATMslot/subslot/port
```

Where:

- *slot*—Specifies the slot number of the VWIC/HWIC previously assigned to the AIM for ATM card.
- *subslot*—Specifies the subslot number of the VWIC/HWIC previously assigned to the AIM for ATM card.
- ***port***—Specifies the port on the VWIC/HWIC previously assigned to the AIM for ATM card.

For example, the following command configures the VWIC/HWIC in logical slot 0 (physical slot 0), subslot 0, port 1 located on the motherboard of the Cisco 3825 router to be used for ATM traffic:

```
Router(config)# interface ATM0/2/0
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 9 To create an ATM path on the UMTS Iub interface, enter the following command:

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

Step 10 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-if)# umts-iub local ip-address port
```

Step 11 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-if)# umts-iub remote ip-address port
```

Step 12 Create an ATM permanent virtual circuit (PVC):

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

Where:

- *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 Q.2931 signaling ATM adaptation layer (QSAAL) encapsulation type.

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 3825 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 3825 router as well.

Step 13 Configure the ATM adaptation layer (AAL) and encapsulation type to AAL0 encapsulation.

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

Where ***aal-encap*** specifies the ATM adaptation layer (AAL) and encapsulation type.

For example, the following command specifies the AAL as AAL0:

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

Step 14 Create another ATM permanent virtual circuit (PVC):

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

Where:

- *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 theQ.2931 signaling ATM adaptation layer (QSAAL) encapsulation type.

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 15 Return to Step 1 to configure the second port of the Cisco 2-port T1/E1-RAN interface card and the ports on additional Cisco 2-port T1/E1-RAN interface cards.

Step 16 Exit the interface configuration mode.

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

Configuring Redundancy

The Cisco 3825 router can be used either in a redundant configuration (preferable) or as a standalone device.

Note Before implementing redundancy, you must disable extended availability drop-and-insert (EADI) capabilities on the router using the **diable-eadi** command in the global configuration mode.

Redundant Cisco 3825 Routers

Use the following instructions to configure the Cisco 3825 router for redundancy. For redundancy, the Cisco 3825 router makes use of the existing HSRP feature. However, additional controls are needed for the Cisco 3825 router. In a redundant configuration, the router must track the status of the health and revertive loopback interfaces as well as the backhaul and shorthaul interfaces. 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 3825 router for use in a redundant configuration, follow these steps while in the global configuration mode:

Step 1 First configure the shorthaul loopback interfaces (loopback 103).

Note The loopback interface is software-only, virtual interface that emulates an interface that is always up. The interface number is the number of the loopback interface that you want to create or configure.

```
Router(config)# interface loopback interface
```

For example, the following command specifies the loopback interface for shorthaul as 103:

```
Router(config)# interface loopback Loopback103
```

Step 2 Enter the ip address and subnet mask for the shorthall loopback interface:

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

Step 3 Exit the interface configuration mode.

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

Step 4 To go to the redundancy mode, enter the **redundancy** command:

```
Router(config)# redundancy
```

Step 5 In the redundancy mode, enter the y-cable mode:

```
Router(config-r)# mode y-cable
```

Step 6 To enable the GSM redundancy, enter the **standby gsm-redundancy** command:

```
Router(config-r)# standby gsm-redundancy
```

Step 7 Specify the interface to be used for backhauling.

```
Router(config-r-y)# standby use-interface interface backhaul
```

Note The interface that you specify for the backhaul must be a Multi-Link Point-to-Point Protocol (MLPPP) interface. If you want to use a serial interface as the backhaul, you must first configure that interface to be part of an MLPPP bundle. The interface that you specify for the backhaul interface should match one of those that you configured and tracked in the "Configuring Multilink Backhaul Interface" section on page 4-15.

For example, the following command specifies the multilink interface for backhaul:

```
Router(config-r-y)# standby use-interface Multilink5 backhaul
```

Step 8 Specify the interface to be used for shorthaul.

```
Router(config-r-y)# standby use-interface interface shorthaul
```

Note The interface that you specify for the shorthaul interface should match the one that you configured in the Step 1.

For example, the following command specifies the loopback interface for shorthaul:

```
Router(config-r-y)# standby use-interface Loopback103 shorthaul
```

Step 9 Exit the y-cable configuration mode.

```
Router(config-r-y)# exit
```

Step 10 Exit the redundancy configuration mode.

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

Step 11 Specify the Gigabit Ethernet interface to be configured (see "Configuring Gigabit Ethernet Interfaces" section on page 4-8 for more details).

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

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

For example, the following command specifies the Gigabit Ethernet interface in slot 0 on port l:

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)#
```

Step 12 Enable HSRP, and assign an IP address to the virtual router. This address is the same for both the active and standby routers.

Note In redundant configurations, the Cisco 3825 router uses HSRP to control the active and standby routers. To use HSRP, you must configure the standby priority attributes and the IP address of the virtual router. Priority is determined first by the configured priority value, and the IP address. In each case, a higher value has greater priority.

```
Router(config-if)# standby [group-number] ip-address [secondary]
```

Where:

- *group-number*—(Optional) Group number on the interface to which the timers apply. The default is 0.
- *ip-address*—(Optional) IP address of the Hot Standby router interface.
- **secondary**—(Optional) Indicates the IP address is a secondary Hot Standby router interface. Useful on interfaces with primary and secondary addresses; you can configure primary and secondary HSRP addresses.

For example, the following command specifies the hot standby group 1 with the IP address as 55.0.0.10:

```
Router(config-if)# standby 1 ip 55.0.0.10
```

Step 13 To configure the time between "hello packets" and the time before other routers declare the active Hot Standby or standby router to be down, use the **standby timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command. Indicate the hot standby group and timers to be configured.

```
Router(config-if)# standby [group-number] timers [msec] hellotime [msec] holdtime
```

Where:

- *group-number*—(Optional) Group number on the interface to which the timers apply. The default is 0.
- **msec**—(Optional) Interval in milliseconds. Millisecond timers allow for faster failover.

- *hellotime*—Hello interval (in seconds). This is an integer from 1 to 254. The default is 3 seconds. If the msec option is specified, hello interval is in milliseconds. This is an integer from 15 to 999.
- *holdtime*—Time (in seconds) before the active or standby router is declared to be down. This is an integer from x to 255. The default is 10 seconds. If the msec option is specified, holdtime is in milliseconds. This is an integer from y to 3000.

  Where:

  – x is the hellotime + 50 milliseconds, then rounded up to the nearest 1 second
  – y is greater than or equal to 3 times the hellotime and is not less than 50 milliseconds.

For example, the following command specifies the hot standby group 1 with the timers set between 1 and 3 seconds:

```
Router(config-if)# standby 1 timers 1 3
```

Step 14 To configure HSRP preemption and preemption delay, use the **standby preempt** command in interface configuration mode. To restore the default values, use the **no** form of this command.

Note Without preemption, a standby router will transition to the active state only if HSPR "hello packets" cease. In a RAN-O solution, you may sometimes want a switchover to occur in the absence of a router GE failure; therefore, you need to configure preemption.

```
Router(config-if)# standby [group-number] preempt [delay{minimum delay|reload delay|sync
delay}]
```

Where:

- *group-number*—(Optional) Group number on the interface to which the other arguments in this command apply.
- *delay*—(Optional) Required if either the **minimum**, **reload**, or **sync** keywords are specified.
- **minimum** *delay*—(Optional) Specifies the minimum delay period in delay seconds. The delay argument causes the local router to postpone taking over the active role for delay (minimum) seconds since that router was last restarted. The range is from 0 to 3600 seconds (1 hour). The default is 0 seconds (no delay).
- **reload** *delay*—(Optional) Specifies the preemption delay period after a reload only. This delay period applies only to the first interface-up event after the router has reloaded.
- **sync** *delay*—(Optional) Specifies the maximum synchronization period for IP redundancy clients in delay seconds.

For example, the following command specifies the hot standby group 1 with preempt:

```
Router(config-if)# standby 1 preempt
```

Note The default group number is 0. The default delay is 0 seconds; if the router wants to preempt, it will do so immediately. By default, the router that comes up later becomes the standby.

Step 15 To configure the name of the standby group, use the **standby name** command in interface configuration mode. To disable the name, use the **no** form of this command.

```
Router(config-if)# standby [group-number] name [group-name]
```

Where:

- *group-number*—Specifies the standby group number.
- *group-name*—Specifies the name of the standby group.

For example, the following command specifies the hot standby group name as *one*:

```
Router(config-if)# standby 1 name_one
```

Note Typically, only one GE is used in a RAN-O solution. So, the command must be **standby 1 name_one**.

Caution If you omit the *group-name* or if you enter a group name that does not begin with one or two, the configuration will fail and there will be a mismatch in the information displayed by the **show redundancy** and **show standby** commands.

Step 16 To configure HSRP to track an object and change the Hot Standby priority based on the state of the object, use the **standby track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

Note When you use the Cisco 3825 router in a RAN-O solution, you must configure the GE interface to track the multilink interface and the loopback interface.

```
Router(config-if)# standby [group-number] track interface-type interface-number
[interface-priority]
```

Where:

- *group-number*—(Optional) Group number to which the tracking applies.
- *interface-type*—Interface type (combined with interface number) that will be tracked.
- *interface-number*—Interface number (combined with interface type) that will be tracked.
- ***interface-priority***—(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The default value is 10.

For example, the following command specifies the hot standby group 1 to track Loopback 103 interface:

```
Router(config-if)# standby 1 track Loopback103
```

Note In redundant configurations, you should issue **standby track** commands for both the health interface (loopback101), the revertive interface (loopback102), the backhaul interface (multilink1), and shorthaul interface (loopback 103). The decrement values *must* be as follows: 10 for the multilink, GE, and health interfaces; 5 for the revertive interface.

Step 17 Continue to configure HSRP to track Multilink1 and Loopback103 if needed.

Step 18 Specify a priority of 100.

```
Router(config-if)# standby group priority 100
```

Note If you are using the Cisco 3825 in a redundant configuration, you must also set the keepalives under the GE interface to 1.

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

Standalone Cisco 3825 Router

The Cisco 3825 router has relays that work with a special y-cable for redundancy and that are controlled by HSRP. You can, however, use the Cisco 3825 as a standalone device. If you choose not to use the Cisco 3825 in a redundant configuration, you should *not* configure HSRP and you must manually control the relays of the Cisco 2-port T1/E1-RAN card.

To manually set the relays to open or closed, follow these steps, while in the global configuration mode:

Step 1 To go to the redundancy mode, enter redundancy mode:

```
Router(config)# redundancy
```

Step 2 In the redundancy mode, enter the y-cable mode:

```
Router(config-r)# mode y-cable
```

Step 3 Specify that the router is to be used as a standalone device. This command closes the relays.

```
Router(config-r-y)# standalone
```

Step 4 Exit y-cable configuration mode.

```
Router(config-r-y)# exit
```

To verify the status of the relays on an Cisco 3825 router, use the **show controllers** command.

Configuring for SNMP Support

Use the following instructions to configure for Simple Network Management Protocol (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 3825 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]
```

Where:

- *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
```

Where *length* is the 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]
```

Where:

- ***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 3825 Mobile Wireless Edge Router RAN-O 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]
```

Where:

- *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 SNMP used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword. If you use the version keyword, one of the following must be specified:
  - **1**—SNMPv1. This option is not available with informs.
  - **2c**—SNMPv2C.
  - **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword:

    –**auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication

    –**noauth** (Default). The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified.

    –**priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
- ***community-string***—Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command before using the **snmp-server host** command.
- **udp-port port**—UDP port of the host to use. The default is 162.
- ***notification-type***—(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords:
  - **aaa_server**—Enable SNMP AAA Server traps.
  - **atm**—Enable SNMP atm Server traps.
  - **ccme**—Enable SNMP ccme traps.
  - **cnpd**—Enable NBAR Protocol Discovery traps.
  - **config**—Enable SNMP config traps.
  - **config-copy**—Enable SNMP config-copy traps.
  - **cpu**—Allow cpu related traps.
  - **dial**—Enable SNMP dial control traps.
  - **dnis**—Enable SNMP DNIS traps.
  - **ds0-busyout**—Enable ds0-busyout traps.
  - **ds1**—Enable SNMP DS1 traps.
  - **ds1-loopback**—Enable ds1-loopback traps.
  - **ds3**—Enable SNMP DS3 traps.
  - **dsp**—Enable SNMP dsp traps.
  - **eigrp**—Enable SNMP EIGRP traps.
  - **entity**—Enable SNMP entity traps.
  - **envmon**—Enable SNMP environmental monitor traps.
  - **flash**—Enable SNMP FLASH notifications.
  - **frame-relay**—Enable SNMP frame-relay traps.
  - **hsrp**—Enable SNMP HSRP traps.
  - **icsudsu**—Enable SNMP ICSUDSU traps.

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

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

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

Step 7 Exit the global configuration mode.

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

Configuring Inverse Multiplexing over ATM (IMA)

A new feature, Inverse Multiplexing over ATM (IMA) interface as a shorthaul has been implemented in Cisco IOS Release 12.4(4)MR. With this feature, you can now configure existing UMTS commands on IMA interfaces. No new commands are added for this new feature. Only previously existing Cisco IOS commands have been added for this feature (see Appendix A, "Cisco 3825 Mobile Wireless Edge Router RAN-O Command Reference" for detailed command information).

Inverse multiplexing provides the capability to transmit and receive a single high-speed data stream over multiple slower-speed physical links. In inverse multiplexing over ATM (IMA), the originating stream of ATM cells is divided so that complete ATM cells are transmitted in round-robin order across the set of ATM links. IMA is supported on the Cisco 2-port T1/E1-RAN card on the Cisco 3825 router.

Note With Cisco IOS Release 12.4(16)MR1 and later, the Cisco 3825 router supports the AIM-ATM-8 card. The Cisco 3825 router supports up to 12 ATM ports with the AIM-ATM-8 card installed in slot 0 and up to 8 ATM ports for AIM with the AIM-ATM-8 card installed in slot 1.

The AIM for ATM card (AIM-ATM) supports up to four independent ATM links.

To determine which AIM for ATM card is installed in your router, use the **show diagnostics** command in privileged EXEC mode.

To configure a Cisco 3825 router for IMA, 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 atmslot/subslot/port
```

Where:

- *slot*—Specifies the slot number of the VWIC/HWIC previously assigned to the AIM for ATM (Step 2 of the "Configuring UMTS Links" procedure on page 4-24).
- *subslot*—Specifies the subslot number of the VWIC/HWIC previously assigned to the AIM for ATM card (Step 2 of the "Configuring UMTS Links" procedure on page 4-24).
- *port*—Specifies the port on the VWIC/HWIC previously assigned to the AIM for ATM card (Step 3 of the "Configuring UMTS Links" procedure on page 4-24).

For example, the following command configures the VWIC/HWIC in logical slot 0 (physical slot 0), subslot 0, port 1 located on the motherboard of the Cisco 3825 router to be used for ATM traffic:

```
Router(config)# interface ATM0/2/0
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 2 Disable the IP address configuration for the physical layer interface. This and other protocol parameters should be configured on the IMA interface.

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

Step 3 Disable the Interim Local Management Interface (ILMI) keepalive parameters.

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

Step 4 Specify the link that is included in an IMA group.

```
Router(config-if)# ima-group group-number
```

Where *group-number* specifies the group number of the IMA group.

For example, the following command specifies the group number of the IMA group as 0:

```
Router(config-if)# ima-group 0
```

Step 5 Randomize the ATM cell payload frames.

```
Router(config-if)# scrambling-payload
```

Step 6 Perform Steps 1 to 5 to add another member link.

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

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

Where:

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

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

```
Router(config-if)# interface ATM0/IMA0
```

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

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

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

Step 9 Specify the ATM bandwith as dynamic.

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

Step 10 Create an ATM path on the UMTS Iub interface, enter the following command:

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

Step 11 Disable the Interim Local Management Interface (ILMI) keepalive parameters.

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

Step 12 Create an ATM PVC:

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

Where:

- *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 theQ.2931 signaling ATM adaptation layer (QSAAL) encapsulation type.

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 3825 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 3825 router as well.

Step 13 Configure the AAL and encapsulation type to AAL0 encapsulation.

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

Where ***aal-encap*** specifies the AAL and encapsulation type.

For example, the following command specifies the AAL as AAL0:

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

Step 14 Perform Steps 12 and 13 to add another ATM PVC.

Step 15 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-if)# umts-iub local ip-address port
```

For example, the following command configures the **umts-iub local** interface with an IP address and port of 20.20.20.21 6666:

```
Router(config-if)# umts-iub local 20.20.20.21 6666
```

Step 16 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-if)# umts-iub remote ip-address port
```

For example, the following command configures the **umts-iub remote** interface with an IP address and port of 20.20.20.20 6666:

```
Router(config-if)# umts-iub remote 20.20.20.20 6666
```

Step 17 Exit the interface configuration mode.

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

Configuring PVC Routing (HSDPA Offload)

A new feature, PVC Routing has been implemented in Cisco IOS Release 12.4(4)MR. With this feature, you can now off load PVC traffic from a physical ATM shorthaul to an alternate backhaul. For each alternate backhaul, you will need to create a logical shorthaul by creating an ATM sub-interface. Traffic from the PVCs configured under this logical shorthaul will go through the corresponding alternate backhaul. Three new commands are added using the Sub-interface Configuration mode for this new feature: **atm umts**, **umts local**, and **umts remote** (see Appendix A, "Cisco 3825 Mobile Wireless Edge Router RAN-O Command Reference" for detailed command information).

To configure a Cisco 3825 router for PVC Routing, follow these steps while in the global configuration mode:

Step 1 First, add the Gigabit Ethernet interfaces by specifying the port adapter type and the location of the interface to be configured.

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

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

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

```
Router(config)# interface gigabitethernet 0/0
```

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

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

For example, the following command specifies the IP address 192.168.1.1 and subnet mask 255.255.255.0:

```
Router(config-if)# interface ip address 192.168.1.1 255.255.255.0
```

Step 3 Specify the duplex operation.

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

For example, the following command specifies the duplex operation as auto:

```
Router(config-if)# duplex auto
```

Step 4 Specify the speed.

```
Router(config-if)# speed [auto | 1000 | 100 | 10]
```

For example, the following command specifies the speed as auto:

```
Router(config-if)# speed auto
```

Step 5 Exit the interface configuration mode.

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

Step 6 Enter interface configuration mode and specify the location of the interface.

```
Router(config)# interface atmslot/subslot/port
```

Where:

- *slot*—Specifies the slot number of the VWIC/HWIC previously assigned to the AIM for ATM (Step 2 of the "Configuring UMTS Links" procedure on page 4-24).
- *subslot*—Specifies the subslot number of the VWIC/HWIC previously assigned to the AIM for ATM card (Step 2 of the "Configuring UMTS Links" procedure on page 4-24).

- *port*—Specifies the port on the VWIC/HWIC previously assigned to the AIM for ATM card (Step 3 of the "Configuring UMTS Links" procedure on page 4-24).

For example, the following command configures the VWIC/HWIC in logical slot 0 (physical slot 0) port 1 located on the motherboard of the Cisco 3825 router to be used for ATM traffic:

```
Router(config)# interface ATM0/2/0
Router(config-if)#
```

Step 7 Disable the IP address configuration for the physical layer interface. This and other protocol parameters should be configured on the IMA interface.

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

Step 8 Disable the Interim Local Management Interface (ILMI) keepalive parameters.

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

Step 9 Specify the link that is included in an IMA group.

```
Router(config-if)# ima-group group-number
```

Where *group-number* specifies the group number of the IMA group.

For example, the following command specifies the group number of the IMA group as 0:

```
Router(config-if)# ima-group 0
```

Step 10 Randomize the ATM cell payload frames.

```
Router(config-if)# scrambling-payload
```

Step 11 Specify the slot location and port of IMA interface group.

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

Where:

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

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

```
Router(config-if)# interface ATM0/IMA0
```

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

Step 12 Create an ATM path on the UMTS Iub interface, enter the following command:

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

Step 13 Disable the ILMI keepalive parameters.

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

Step 14 Create an ATM PVC:

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

Where:

- *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 theQ.2931 signaling ATM adaptation layer (QSAAL) encapsulation type.

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 3825 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 3825 router as well.

Step 15 Configure the AAL and encapsulation type to AAL0 encapsulation.

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

Where ***aal-encap*** specifies the AAL and encapsulation type.

For example, the following command specifies the AAL as AAL0:

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

Step 16 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-if)# umts-iub local ip-address port
```

For example, the following command configures the **umts-iub local** interface with an IP address and port of 20.20.20.21 6666:

```
Router(config-if)# umts-iub local 20.20.20.21 6666
```

Step 17 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-if)# umts-iub remote ip-address port
```

For example, the following command configures the **umts-iub remote** interface with an IP address and port of 20.20.20.20 6666:

```
Router(config-if)# umts-iub local 20.20.20.20 6666
```

Step 18 Exit the interface configuration mode.

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

Step 19 Specify the ATM/IMA interface that the PVCs will be assigned to and enter the sub-interface mode.

```
Router(config)# interface ATMslot/IMA<group-number>[.<subinterface-number> {multipoint
point-to-point}]
```

Where:

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

For example, the following command specifies the slot number as 0 and the group number as 0.1 for multipoint:

```
Router(config)# interface ATM0/IMA0.1 multipoint
```

Step 20 Create an ATM path on the UMTS Iub interface, enter the following command:

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

Step 21 Create an ATM PVC:

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

Where:

- *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 theQ.2931 signaling ATM adaptation layer (QSAAL) encapsulation type.

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 1and a VCI of 200:

```
Router(config-subif)# pvc 1/200
```

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 3825 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 3825 router as well.

Step 22 Configure the AAL and encapsulation type to AAL0 encapsulation.

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

Where ***aal-encap*** specifies the AAL and encapsulation type.

For example, the following command specifies the AAL as AAL0:

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

Step 23 Exit the interface atm configuration mode.

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

Step 24 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
```

For example, the following command configures the **umts-iub local** interface with an IP address of 192.168.10.2 and a port of 6000:

```
Router(config-subif)# umts-iub local 192.168.10.2 6000
```

Step 25 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
```

For example, the following command configures the **umts-iub remote** interface with an IP address of 192.168.10.1 and a port of 6000:

```
Router(config-subif)# umts-iub remote 192.168.10.1
```

Note In the above procedure, traffic for PVC 1/200 will be off-loaded to the alternate backhaul (192.168.10.2 — 192.168.10.1).

Step 26 Exit the sub-interface configuration mode.

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

Note For more information about PVC Routing, see the "Permanent Virtual Circuit (PVC) Routing" section on page 1-30. Example output from the show umts peer command as well as specific behavior changes are described.

Configuring UMTS QoS

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 Interface Configuration command: **umts-iub set dscp** (see Appendix A, "Cisco 3825 Mobile Wireless Edge Router RAN-O Command Reference" for detailed command information). These new commands allow you to perform the following:

- UMTS Shorthaul Interface
  - Set the default description value to tag the backhaul packet including peering and data generated from the shorthaul in a UMTS Iub configuration.
  - Set the description value in the UMTS Iub configuration such that it overwrites the default value defined previously. It is also used to tag the peering backhaul packet.
- PVC of a UMTS Shorthaul Interface
  - Set the description value in the UMTS Iub configuration such that it overwrites the default value defined previously. It is also used to tag the backhaul packet generated from traffic from the PVC.
- GSM Shorthaul Interface
  - Set the description 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 ATM0/0/0 and ATM0/0/1 will go to the priority queue and PVC 2/2 of ATM0/0/0 and ATM0/0/1 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
```

Where **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 cs2
```

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
```

Where *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
```

Where *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 4-47.

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.

Specify the Location of the Interface

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

```
Router(config)# interface atmslot/subslot/port
```

For example, the following command specifies the location of the interface as ATM0/0.

```
Router(config# interface atm0/0/0
```

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)# no atm ilmi-keepalive
```

Step 5 Create an ATM PVC:

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

Where:

- *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 theQ.2931 signaling ATM adaptation layer (QSAAL) encapsulation type.

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 3825 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 3825 router as well.

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

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

Where ***aal-encap*** specifies the AAL and encapsulation type.

For example, the following command specifies the 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)# umts-iub set dscp value
```

Where ***value*** is 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 16
```

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
```

Where ***value*** is 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)# umts-iub set dscp 16
```

Step 10 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-if)# umts-iub local ip-address port
```

For example, the following command configures the **umts-iub local** interface with an IP address and port of 20.20.20.21 6666:

```
Router(config-if)# umts-iub local 20.20.20.21 6666
```

Step 11 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-if)# umts-iub remote ip-address port
```

For example, the following command configures the **umts-iub remote** interface with an IP address and port of 20.20.20.20 6666:

```
Router(config-if)# umts-iub remote 20.20.20.20 6666
```

Step 12 Perform Steps 1 to 7 for ATM0/0/1 with a UMTS DSCP of 8.

Step 13 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
```

Where ***value*** is 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)# umts-iub set dscp 16
```

Step 14 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-if)# umts-iub local ip-address port
```

For example, the following command configures the **umts-iub local** interface with an IP address and port of 20.20.20.21 8888:

```
Router(config-if)# umts-iub local 20.20.20.21 8888
```

Step 15 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-if)# umts-iub remote ip-address port
```

For example, the following command configures the **umts-iub remote** interface with an IP address and port of 20.20.20.20 8888:

```
Router(config-if)# umts-iub remote 20.20.20.20 8888
```

Step 16 Exit the interface configuration mode.

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

Assigning a QoS Boilerplate to an Interface

Use the following instructions to assign a quality of service (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 multiclass multilink PPP (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.

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 assign a QoS boilerplate to a multilink interface, follow these steps, while in the global configuration mode.

Step 1 Enter the interface configuration mode.

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

Where *group-number* is the number of the multilink bundle.

For example, the following command creates a multilink bundle 2:

```
Router(config)# interface multilink2
Router(config-if)#
```

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

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

For example, the following command creates a an IP address of 20.20.20.21 and a subnet mask of 255.255.255.0:

```
Router(config-if)# ip address 20.20.20.21 255.255.255.0
```

Step 3 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 4 Change the length of time for which data is used, enter the following command:

```
Router(config-if)# load-interval seconds
```

Where *seconds* is the 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).

For example, the following command has the length of time set at 30 seconds:

```
Router(config-if)# load-interval 30
```

Step 5 Disable the keepalive parameters.

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

Step 6 Disable the Cisco Discovery Protocol (CDP) on the interface.

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

Step 7 To configure PFC on the router, enter the following command:

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

Where:

- **request**—The PFC option is included in outbound configuration requests.
- **forbid**—The PFC option is not sent in outbound configuration requests, and requests from a remote peer to add the PFC option are not accepted.

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

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

Step 8 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 9 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 10 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 11 Enable multilink PPP operation.

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

Step 12 Enable real-time packet interleaving.

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

Step 13 Specify an identification number for the multilink interface.

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

Where *group-number* is the 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 14 Configure a fragment delay.

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

Where *delay* is optional and configures a maximum fragment delay. If, for example, you want a voice stream to have a maximum bound on delay of 20 milliseconds (ms) and you specify 20 ms using this command, MLPPP will choose a fragment size based on the configured value.

For example, the following command configures the delay from 0 to 1 millisecond:

```
Router(config-if)# ppp multilink delay 0 1
```

Step 15 Enable MCMP.

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

Step 16 Specify the percent of the interface bandwidth allocated for LLQ.

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

Where *percent* is the 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 17 Assign the QoS boilerplate to the multilink interface.

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

Where *policy_name* is 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 18 Set the size of the output queue.

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

Where:

- *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 4-47 for more information).

Step 19 Enable 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
```

Note In the previous procedure, PVC 2/1 of ATM0/0/0 and ATM0/0/1 will go to the priority queue and PVC 2/2 of ATM0/0/0 and ATM0/0/1 will be considered the best effort traffic and will go to the Weighted Fair Queue.

Configuring UMTS Congestion Management Control

A new feature for Cisco IOS Release 12.4(4)MR1, UMTS Congestion Management Control has been implemented. With this feature, you can now configure the UMTS congestion based on priority.

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 3825 router for UMTS Congestion Control for IMA, follow these steps while in the Privileged EXEC mode:

Step 1 Enter global configuration mode from the terminal.

```
Router# configure terminal
```

Step 2 Enter interface configuration mode and specify the location of the interface.

- *slot*—Specifies the slot number of the VWIC/HWIC previously assigned to the AIM for ATM (Step 2 of the "Configuring UMTS Links" procedure on page 4-24).
- *subslot*—Specifies the subslot number of the VWIC/HWIC previously assigned to the AIM for ATM card (Step 2 of the "Configuring UMTS Links" procedure on page 4-24).
- *port*—Specifies the port on the VWIC/HWIC previously assigned to the AIM for ATM card (Step 3 of the "Configuring UMTS Links" procedure on page 4-24).

For example, the following command configures the VWIC/HWIC in logical slot 0 (physical slot 0) port 1 located on the motherboard of the Cisco 3825 router to be used for ATM traffic:

```
Router(config)# interface ATM0/2/0
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 3 Disable the IP address configuration for the physical layer interface. This and other protocol parameters should be configured on the IMA interface.

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

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

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

Step 5 Specify the link that is included in an IMA group.

```
Router(config-if)# ima-group group-number
```

Where *group-number* specifies the group number of the IMA group.

For example, the following command specifies the group number of the IMA group as 0:

```
Router(config-if)# ima-group 0
```

Step 6 Randomize the ATM cell payload frames.

```
Router(config-if)# scrambling-payload
```

Step 7 Perform Steps 1 to 5 to add another member link.

Step 8 Specify the slot location and port of IMA interface group.

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

Where:

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

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

```
Router(config-if)# interface ATM0/IMA0
```

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

Step 9 Disable the IP address configuration for the physical layer interface.

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

Step 10 Specify the ATM bandwidth as dynamic.

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

Step 11 Create an ATM path on the UMTS Iub interface, enter the following command:

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

Step 12 Disable the ILMI keepalive parameters.

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

Step 13 Create an ATM PVC:

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

Where:

- *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**—See Note.

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 3825 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 3825 router as well.

Step 14 Configure the AAL and encapsulation type to AAL0 encapsulation.

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

Where ***aal-encap*** specifies the AAL and encapsulation type.

For example, the following command specifies the AAL as AAL0:

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

Step 15 To set the UMTS Congestion priority for protected, enter the following command.

```
Router(config-if-atm-vc)# umts-iub congestion priority protected
```

Step 16 To set the UMTS Congestion priority to level 4, enter the following command.

```
Router(config-if-atm-vc)# umts-iub congestion priority 4
```

Step 17 To enable the UMTS Congestion Control under UMTS shorthaul interface, enter the following command.

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

Step 18 To set the DSCP value used as the interface default DSCP value to tag the backhaul packet, use the following command:

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

Where ***value*** is a number chosen to represent that packet of traffic.

For example, the following command specifies the number 8 for the packet of traffic for the umts-iub interface:

```
Router(config-if)# umts-iub set dscp 8
```

Step 19 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 peering dscp value
```

Where ***value*** is 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)# umts-iub set peering dscp 16
```

Step 20 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-if)# umts-iub local ip-address port
```

For example, the following command configures the **umts-iub local** interface with an IP address and port of 20.20.20.21 6666:

```
Router(config-if)# umts-iub local 20.20.20.21 6666
```

Step 21 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-if)# umts-iub remote ip-address port
```

For example, the following command configures the **umts-iub remote** interface with an IP address and port of 20.20.20.20 6666:

```
Router(config-if)# umts-iub local 20.20.20.20 6666
```

Step 22 Exit the interface configuration mode.

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

Configuring Satellite Support

To support the configuration of a network when satellites are employed, you must implement a configurable jitter buffer and a tunable retransmission timer of repetitive sub-rates to overcome the network latency and satellite signal fade.

Use the following instructions to perform a GSM-Abis configuration with satellite support on the Cisco 2-port T1/E1-RAN interface card located in the Cisco 3825 router by entering the following Cisco IOS commands at the router prompt.

You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

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

To configure the GSM-Abis attributes with satellite support, 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 4-20).

Step 2 To configure the jitter buffer, enter the following command including the value of the jitter buffer.

```
Router(config-if)# gsm-abis jitter value ms
```

Where ***ms*** is the value range in milliseconds of the jitter buffer. The default is 4 ms.

For example, the following command configures the **gsm-abis jitter** buffer to 10 ms:

```
Router(config-if)# gsm-abis jitter 10
```

Step 3 To configure the tunable retransmission timer, enter the following command including the value in milliseconds to retransmit.

```
Router(config-if)# gsm-abis retransmit value
```

Where ***value*** is the sample delay which is a value range of the retransmission of 100 ms to 5100 ms in 20 ms intervals. For example, if the value is 5, then the amount of time in ms would be calculated as 5 times 20 ms or a total of 100 ms as the retransmit time.

For example, the following command configures the **gsm-abis retransmit** timer to a value of 5 or 100 ms:

```
Router(config-if)# gsm-abis retransmit 5
```

Configuring Graceful Degradation

A local Cisco 3825 router detects congestion on the backhaul by measuring its transmit jitter buffer level. If the transmit jitter buffer shrinks, it means that the backhaul packets are not arriving fast enough to fill the transmit jitter buffer indicating congestion. You should set the congestion abatement detection level at which a remote router will stop suppressing these timeslots.

Use the following instructions to configure graceful degradation on the Cisco 3825 router by entering the following Cisco IOS commands at the router prompt.

You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

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

To configure graceful degradation, follow these steps while in the global configuration mode:

Step 1 Perform Steps 1 through 10 as described in the previous procedure (see the "Configuring GSM-Abis Links" procedure on page 4-20).

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
```

Where ***ms*** is 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
```

Where ***ms*** is 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
```

Where ***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 3825 router, to prevent the loss of the router configuration, you must store the configuration changes by saving it to nonvolatile random-access memory (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
```

Example Configurations

The following examples show sample configurations for the:

- BTS/Node-B side of the Cisco 3825 Mobile Wireless Edge Router
- Base Station Controller/Radio Network Controller (BSC/RNC) side of the Cisco 3825 Mobile Wireless Edge Router

BTS/Node-B Configuration

```
!
version 12.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname hostname !--- Enter <hostname> here
!
boot-start-marker
boot system flash slot0: !--- Image Name
boot-end-marker
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
logging buffered 1000000 debugging
enable password !--- Set the ENABLE password here
!
no aaa new-model
!
resource manager
!
clock timezone EST -5 !--- Example of setting time zone
!
```

```
redundancy
     mode y-cable
         standalone
!
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 0/1/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip dhcp use vrf connected
!
!
no ip domain lookup
!
!
!
!
!--- The use of CRC4 or NO-CRC4 is dependent on the configuration of the end user
equipment.
!
!
!
controller E1 0/0/0
     framing NO-CRC4
     clock source internal
     channel-group 0 timeslots 1-31
     description Short Haul Abis E1 NO-CRC4 framing
!
controller E1 0/0/1
     clock source internal
     channel-group 0 timeslots 1-31
     description Short Haul Abis E1 CRC4 framing (default)
!
controller E1 0/1/0
     channel-group 0 timeslots 1-31
     description Backhaul IP E1
!
controller E1 0/1/1
     mode atm aim 1
     description Short Haul Iub E1
!
controller E1 0/2/0
     mode atm aim 1
     description Short Haul Iub E1
     clock source internal
!
class-map match-any abis
     match ip dscp 15!
!
policy-map llq-policy
     class abis
         priority percent 99
     class class-default
         bandwidth remaining percent 1
         queue-lmit 45
!
!
interface Loopback0
     description O&M IP Globally Routable
```

```
     ip address 10.10.10.2 255.255.255.255
!
interface Loopback1
     description Loopback IP for Unnumbered
     ip address 172.168.1.2 255.255.255.252
!
interface Multilink1
     description MLPPP IP interface for IP backhaul bundle
     ip unnumbered Loopback1
     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 interleave
     ppp multilink group 1
     ppp multilink fragment delay 0 1
     ppp multilink multiclass
     hold-queue 50 out
     max-reserved-bandwidth 100
     service-policy output llq-policy
     ip rtp header-compression ietf-format
!
interface GigabitEthernet0/0
     no ip address
     shutdown
     duplex auto
     speed auto
!
interface Serial0/0/0:0
     no ip address
     no keepalive
     description GSM Abis interface
     encapsulation gsm-abis
     gsm-abis local 172.168.1.2 3334 !--- Port numbers must be even
     gsm-abis remote 172.168.1.1 3334 !--- Port numbers must be even
!
interface GigabitEthernet0/1
     no ip address
     shutdown
     duplex auto
     speed auto
!
interface Serial0/0/1:0
     no ip address
     no keepalive
     description GSM Abis interface
     encapsulation gsm-abis
     gsm-abis local 172.168.1.2 3336
     gsm-abis remote 172.168.1.1 3336
!
interface Serial0/1/0:0
     no ip address
     description IP backhaul MLPPP member interface
     encapsulation ppp
     ppp multilink group 1
     max-reserved-bandwidth 100
!
interface ATM0/1/1
     no ip address
```

```
     description Default E1 Iub interface configuration
     scrambling-payload
     no atm ilmi-keepalive
     atm umts-iub
     umts-iub local 172.168.1.2 6000
     umts-iub remote 172.168.1.1 6000
     pvc 1/32 !--- PVCs needed will vary
     encapsulation aal0
     !
     pvc 1/33
     encapsulation aal0
     !
     pvc 1/34
     encapsulation aal0
     !
     pvc 1/35
     encapsulation aal0
     !
     pvc 1/36 qsaal
     !
     pvc 1/37 qsaal
     !
     pvc 1/38 qsaal
     !
     pvc 1/39
     encapsulation aal0
     !
     pvc 1/43 qsaal
     !
     pvc 1/44 qsaal
     !
     pvc 1/45 qsaal
     !
!
interface ATM0/2/0
     no ip address
     description Default Motorola Iub interface configuration
     scrambling-payload
     no atm ilmi-keepalive
     atm umts-iub
     umts-iub local 172.168.1.2 6002
     umts-iub remote 172.168.1.1 6002
     pvc 1/32 !--- PVCs needed will vary
     encapsulation aal0
     !
     pvc 1/36 qsaal
     !
     pvc 1/37 qsaal
     !
     pvc 1/39
     encapsulation aal0
     !
!
snmp-server community public RO
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran alarm
snmp-server trap link ietf
snmp-server host 10.10.10.10 version 2c v2c
!--- Public and 10.10.10.10 need to be replaced with customer specified values
!
ip classless
!
no ip http server
!
```

```
disable-eadi
!
!
control-plane
!
line con 0
     logging synchronous
line aux 0
line vty 04
     login
     password !--- Set VTY password
!
ntp server W.X.Y.Z !--- Set W.X.Y.Z to the NTP server on the network. This is important so
!that all the MWTM reports sync with the correct time. MWTM should sync to the same NTP
!server.
```

BSC/RNC Configuration

```
!
version 12.4
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname hostname !--- Enter <hostname> here
!
boot-start-marker
boot system flash slot0: !--- Image Name
boot-end-marker
!
card type e1 0 0
card type e1 0 1
card type e1 0 2
logging buffered 1000000 debugging
enable password !--- Set the ENABLE password here
!
no aaa new-model
!
resource manager
!
clock timezone EST -5 !--- Example of setting time zone
!
redundancy
     mode y-cable
         standalone
!
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 0/0/0
network-clock-select 2 E1 0/0/1
network-clock-select 3 E1 0/1/1
network-clock-select 4 E1 0/2/0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip dhcp use vrf connected
!
!
```

```
no ip domain lookup
!
!
!
!
!--- The use of CRC4 or NO-CRC4 is dependent on the configuration of the end user
equipment.
!
!
!
controller E1 0/0/0
     framing NO-CRC4
     clock source internal
     channel-group 0 timeslots 1-31
     description Short Haul Abis E1 NO-CRC4 framing
!
controller E1 0/0/1
     clock source internal
     channel-group 0 timeslots 1-31
     description Short Haul Abis E1 CRC4 framing (default)
!
controller E1 0/1/0
     channel-group 0 timeslots 1-31
     description Backhaul IP E1
!
controller E1 0/1/1
     mode atm aim 1
     description Short Haul Iub E1
!
controller E1 0/2/0
     mode atm aim 1
     description Short Haul Iub E1
!
class-map match-any abis
     match ip dscp 15
!
!
policy-map llq-policy
     class abis
         priority percent 99
     class class-default
         bandwidth remaining percent 1
         queue-lmit 45
!
!
interface Loopback0
     description O&M IP Globally Routable
     ip address 10.10.10.1 255.255.255.255
!
interface Loopback1
     description Loopback IP for Unnumbered
     ip address 172.168.1.1 255.255.255.252
!
interface Multilink1
     description MLPPP IP interface for IP backhaul bundle
     ip unnumbered Loopback1
     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 interleave
     ppp multilink group 1
     ppp multilink fragment delay 0 1
     ppp multilink multiclass
     hold-queue 50 out
     max-reserved-bandwidth 100
     service-policy output llq-policy
     ip rtp header-compression ietf-format
!
interface GigabitEthernet0/0
     description GE interface providing IP connectivity to MWTM server
     ip address W.X.Y.Z A.B.C.D
     speed 1000
     full-duplex
!
interface Serial0/0/0:0
     no ip address
     no keepalive
     description GSM Abis interface
     encapsulation gsm-abis
     gsm-abis local 172.168.1.1 3334 !--- Port numbers must be even
     gsm-abis remote 172.168.1.2 3334 !--- Port numbers must be even
!
interface GigabitEthernet0/1
     no ip address
     shutdown
     duplex auto
     speed auto
!
interface Serial0/0/1:0
     no ip address
     no keepalive
     description GSM Abis interface
     encapsulation gsm-abis
     gsm-abis local 172.168.1.1 3336
     gsm-abis remote 172.168.1.2 3336
!
interface Serial0/1/0:0
     no ip address
     description IP backhaul MLPPP member interface
     encapsulation ppp
     ppp multilink group 1
     max-reserved-bandwidth 100
!
interface ATM0/1/1
     no ip address
     description Default E1 Iub interface configuration
     scrambling-payload
     no atm ilmi-keepalive
     atm umts-iub
     umts-iub local 172.168.1.1 6000
     umts-iub remote 172.168.1.2 6000
     pvc 1/32 !--- PVCs needed will vary
     encapsulation aal0
     !
     pvc 1/33
     encapsulation aal0
     !
     pvc 1/34
     encapsulation aal0
     !
     pvc 1/35
     encapsulation aal0
```

```
     !
     pvc 1/36 qsaal
     !
     pvc 1/37 qsaal
     !
     pvc 1/38 qsaal
     !
     pvc 1/39
     encapsulation aal0
     !
     pvc 1/43 qsaal
     !
     pvc 1/44 qsaal
     !
     pvc 1/45 qsaal
     !
!
interface ATM0/2/0
     no ip address
     description Default Motorola Iub interface configuration
     scrambling-payload
     no atm ilmi-keepalive
     atm umts-iub
     umts-iub local 172.168.1.1 6002
     umts-iub remote 172.168.1.2 6002
     pvc 1/32 !--- PVCs needed will vary
     encapsulation aal0
     !
     pvc 1/36 qsaal
     !
     pvc 1/37 qsaal
     !
     pvc 1/39
     encapsulation aal0
     !
!
snmp-server community public RO
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran alarm
snmp-server trap link ietf
snmp-server host 10.10.10.10 version 2c v2c
!--- Public and 10.10.10.10 need to be replaced with customer specified values
!
ip classless
!
no ip http server
!
disable-eadi
!
!
control-plane
!
line con 0
     logging synchronous
line aux 0
line vty 04
     login
     password !--- Set VTY password
!
ntp server W.X.Y.Z !--- Set W.X.Y.Z to the NTP server on the network. This is important so
!that all the MWTM reports sync with the correct time. MWTM should sync to the same NTP
!server.
```

Monitoring and Managing the Cisco 3825 Router

You can use Cisco's network management applications, such as Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco 3825 router. 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 Cisco 3825 Router for Remote Network Management

To enable remote network management of the Cisco 3825 router, 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 4-8 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 4-33 for more information about configuring Steps 5 through 8 in this procedure.

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

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

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

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

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

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

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

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

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

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

Show Commands for Monitoring the Cisco 3825 Router

To monitor and maintain the Cisco 3825 router, use the following commands:

Command	Purpose
show atm cell-packing	Displays information about Layer 2 transport ATM cell-packing.
show cem circuit	Displays summary information about the CEM circuit state, including controller, interface and AC. Displays specific CEM circuit state, circuit parameters and statistics/counters in detail.
show cem platform	Displays CEM errors and information.
show controllers	Displays all network modules and their interfaces. Displays the status of the VWIC/HWIC relays when a VWIC or HWIC is installed.
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 slot and a port number, statistics for each 15 minute period will be displayed.
show controllers fastethernet slot/port	Displays information about initialization block, transmit ring, receive ring and errors for the Fast Ethernet controller chip.
show controllers gigabitethernet slot/subslot/port	Displays information about initialization block, transmit ring, receive ring, and errors for Gigabit Ethernet interface controllers.
show controllers t1	Displays information about the cable length, framing, firmware, and errors associated with the T1. With the Cisco 3825 router, this command also displays the status of the relays on the VWIC/HWIC.
show gsm traffic	Displays 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.
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]	Displays peering status, statistics, and history of the GSM compression/decompression.

Command	Purpose
show interface *type slot/port*	Displays the configuration and status of the specified interface.
show interfaces fastethernet slot/port	Displays the status of the FE interface.
show interfaces gigabitethernet slot/port	Displays the status and configuration settings of the GE interface.
show ip rtp header-compression	Displays RTP header compression statistics.
show l2tp session	Displays session information about active Layer 2 sessions.
show l2tp tunnel	Displays information about active Layer 2 tunnels.
show mpls l2transport vc	Displays information about Any Transport over MPLS (AToM) virtual circuits (VCs) that have been enabled to route Layer 2 packets on a router.
show network-clocks	Displays the network clocking configuration.
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 redundancy	Displays current redundant setting and recent changes in state.
show standby	Displays HSRP configuration information.
show umts traffic	Displays 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.
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.
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	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 xconnect all	Displays xconnect information.

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.