APPENDIX A

Cisco RAN Service Module Command Reference

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

The following commands have been introduced:

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

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

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

atm umts-iub

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

atm umts-iub [aggnode]

Syntax Description

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

Command Modes Sub-Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

clear gsm-abis

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

clear gsm-abis [serial *number***]**

Syntax Description

type number	(Optional) Interface type and number.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

cdp enable

To enable Cisco Discovery Protocol (CDP) on an interface, use the **cdp enable** command in interface configuration mode. To disable CDP on an interface, use the no form of this command.

cdp enable

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

CDP is enabled by default at the global level and on each supported interface in order to send or receive CDP information. However, some interfaces, such as ATM interfaces, do not support CDP.

Note The **cdp enable**, **cdp timer**, and **cdp run** commands affect the operation of the IP on demand routing feature (that is, the **router odr** Global configuration command). For more information on the **router odr** command, see the "On-Demand Routing Commands" chapter in the *Cisco IOS Command Reference, Volume 2 of 3: Routing Protocols* document.

Examples

In the following example, CDP is disabled on the Ethernet 0 interface only.

```
Router# show cdp
Global CDP information
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
Router# config terminal
Router(config)# interface ethernet 0
Router(config-if)# no cdp enable
```

Related Commands

Command	Description
cdp run	Re-enables CDP on a Cisco device.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
router odr	Enables on-demand routing on a hub router

clear ip rtp header-compression

To clear Real-Time Transport Protocol (RTP) header compression structures and statistics, use the **clear ip rtp header-compression** privileged EXEC command.

clear ip rtp header-compression [*type number***]**

Syntax Description

type number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear umts-iub

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

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

Syntax Description

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

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

gsm-abis congestion abate

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

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

gsm-abis congestion abate [ms]

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to the gsm-abis abate command is set at 250 ms:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# gsm-abis congestion abate 250
Router(config-if)# no keepalive
```

Related Commands

Command	Description
gsm-abis congestion critical	Defines the critical timeslots that are exempt from suppression during congestion onset.
gsm-abis congestion enable	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote when congestion is detected.
gsm-abis congestion onset	Sets the congestion onset detection level at which the remote router will start suppressing all timeslots that are not defined as critical in an effort to alleviate the congestion.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.

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

gsm-abis congestion critical

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

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

gsm-abis congestion critical [timeslot-range]

Syntax Description

timeslot-range	Specifies a value or range of values for time slots that are exempt from suppression during congestion onset. Use a hyphen to indicate a range.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to set the timeslots range:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# gsm-abis congestion critical 2-3
Router(config-if)# no keepalive
```

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.
gsm-abis congestion enable	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote when congestion is detected.
gsm-abis congestion onset	Sets the congestion onset detection level at which the remote router will start suppressing all timeslots that are not defined as critical in an effort to alleviate the congestion.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.

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

gsm-abis congestion enable

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

gsm-abis congestion enable

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

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

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# no keepalive
```

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.
gsm-abis congestion critical	Defines the critical timeslots that are exempt from suppression during congestion onset.
gsm-abis congestion onset	Sets the congestion onset detection level at which the remote router will start suppressing all timeslots that are not defined as critical in an effort to alleviate the congestion.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.

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

gsm-abis congestion onset

Sets the congestion onset detection level at which the remote router will start suppressing all timeslots that are not defined as critical in an effort to alleviate the congestion.

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

gsm-abis congestion onset [ms]

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to set the onset detection level at 50 ms:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis congestion enable
Router(config-if)# gsm-abis congestion onset 100
Router(config-if)# no keepalive
```

Related Commands

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

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

gsm-abis jitter

Sets the amount of transmit jitter delay for the GSM-Abis interface.If the transmit jitter is set to 4 ms, data received on the backhaul with a time equal to 0 milliseconds will be stored in the jitter buffer and transmitted with a time equal to 4 milliseconds. The transmit jitter buffer allows some amount of jitter in the arrival of data on the backhaul to be tolerated without introducing errors into the stream of data.

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

gsm-abis jitter *ms*

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to set the jitter level to 8 ms:

```
Router(config)# interface Serial10/2:0
Router(config-if)# no ip address
Router(config-if)# encapsulation gsm-abis
Router(config-if)# load-interval 30
Router(config-if)# gsm-abis local 10.10.10.2 6661
Router(config-if)# gsm-abis remote 10.10.10.1 5553
Router(config-if)# gsm-abis jitter 8
Router(config-if)# no keepalive
```

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router will stop suppressing timeslots because congestion has been alleviated.
gsm-abis congestion critical	Defines the critical timeslots that are exempt from suppression during congestion onset.
gsm-abis congestion enable	Sets the congestion detection algorithm to monitor the transmit jitter buffer and to send congestion indicator signals to the remote when congestion is detected.
gsm-abis congestion onset	Sets the congestion onset detection level at which the remote router will start suppressing all timeslots that are not defined as critical in an effort to alleviate the congestion.

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

gsm-abis local

To configure the local parameters required to establish an Internet Protocol/User Data Protocol (IP/UDP) backhaul connection, use the **gsm-abis local** Interface configuration command.

gsm-abis local [**ip-address] [***port***]**

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the local parameters:

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

Related Commands

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

gsm-abis remote

To configure the remote parameters required to establish an Internet Protocol/User Data Protocol (IP/UDP) backhaul connection, use the **gsm-abis remote** Interface configuration command.

gsm-abis remote [**ip-address] [***port***]**

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the remote parameters:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis remote 10.10.10.1 5504
```

Related Commands

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

gsm-abis retransmit

To enable retransmission of repetitive subrate sample, use the **gsm-abis retransmit** Interface configuration command. This command is useful when the latency introduced by the characteristics of the backhaul network is excessive. Examples are the use of satellite transmission facilities or multiple router hops on the backhaul network.

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

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how a retransmit delay of 100 ms:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis local 10.10.10.1 5504
Router(config-if)# gsm-abis remote 10.10.10.2 5504
Router(config-if)# gsm-abis retransmit 5
```

Related Commands

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

gsm-abis set dscp

To mark a packet by setting the differential services code point (DSCP) for GSM-Abis, use the **gsm-abis set dscp** Interface configuration command.

gsm-abis set dscp *value*

Note Use this command when configuring GSM shorthaul interfaces.

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to set a retransmit delay of 100 ms:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis local 10.10.10.1 5504
Router(config-if)# gsm-abis remote 10.10.10.2 5504
Router(config-if)# gsm-abis set dscp cs2
```

ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression, use the **ip rtp header-compression** command in interface configuration mode. To disable RTP header compression, use the **no** form of this command.

ip rtp header-compression [**passive** | **iphc-format** | **ietf-format**] [**periodic-refresh**]

no ip rtp header-compression [**passive** | **iphc-format** | **ietf-format**] [**periodic-refresh**]

Syntax Description

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

Defaults

Disabled

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

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can compress IP/User Datagram Protocol (UDP)/RTP headers to reduce the size of your packets. Compressing headers is especially useful for RTP because RTP payload size can be as small as 20 bytes, and the uncompressed header is 40 bytes.

The passive Keyword

By default, the **ip rtp header-compression** command compresses outgoing RTP traffic. If you specify the **passive** keyword, outgoing RTP traffic is compressed only if *incoming* RTP traffic on the *same* interface is compressed. If you do not specify the **passive** keyword, *all* outgoing RTP traffic is compressed.

The **passive** keyword is ignored on PPP interfaces. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

The iphc-format Keyword

The **iphc-format** keyword indicates that the IPHC format of header compression that will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, TCP header compression is also enabled. For this reason, the **ip tcp header-compression** command appears in the output of the **show running-config** command. Since both RTP header compression and TCP header compression are enabled, both UDP packets and TCP packets are compressed.

The **iphc-format** keyword includes checking whether the destination port number is even and is in the ranges of 16,385 to 32,767 (for Cisco audio) or 49,152 to 65,535 (for Cisco video). Valid RTP packets that meet the criteria (that is, the port number is even and is within the specified range) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

The ietf-format Keyword

The **ietf-format** keyword indicates that the IETF format of header compression will be used. For HDLC interfaces, the **ietf-format** keyword compresses only UDP packets. For PPP interfaces, when the **ietf-format** keyword is specified, TCP header compression is also enabled. For this reason, the **ip tcp header-compression** command appears in the output of the **show running-config** command. Since both RTP header compression and TCP header compression are enabled, both UDP packets and TCP packets are compressed.

With the **ietf-format** keyword, any even destination port number higher than 1024 can be used. Valid RTP packets that meet the criteria (that is, the port number is even and is higher than 1024) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.

Note The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format** keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

Support for Serial Lines

RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection.

Unicast or Multicast RTP Packets

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

Examples

The following example enables RTP header compression on the Serial1/0 interface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip rtp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# exit
```

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

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

In the following example, RTP header compression is enabled on the Serial1/0 interface and the optional **periodic-refresh** keyword of the **ip rtp header-compression** command is specified:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format periodic-refresh
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# exit
```

Related Commands

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

ip tcp header-compression

To enable Transmission Control Protocol (TCP) header compression, use the **ip tcp header-compression** command in interface configuration mode. To disable compression, use the **no** form of this command.

ip tcp header-compression [passive] [**iphc-format**] **[ietf-format]**

no ip tcp header-compression [passive] [**iphc-format**] **[ietf-format]**

Syntax Description

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, all TCP packets are compressed.
iphc-format	(Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used.
ietf-format	(Optional) Indicates that the Internet Engineering Task Force (IETF) format of the header compression will be used.

Defaults

Disabled

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

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format is as described in RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. Compressing the TCP header can speed up Telnet connections dramatically.

In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on User Datagram Protocol (UDP) packets or other headers.

Header Compression passive Keyword

By default, the **ip tcp header-compression** command compresses outgoing TCP traffic. This command includes an optional **passive** keyword. If you specify the **passive** keyword, outgoing TCP traffic is compressed only if *incoming* TCP traffic on the *same* interface is compressed. If you do not specify the passive keyword, *all* TCP traffic is compressed.

For PPP interfaces, the passive keyword is ignored. PPP interfaces negotiate the use of header-compression, regardless of whether the passive keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by IPHC format, the default format for PPP interfaces.

Header Compression iphc-format Keyword

This command includes the **iphc-format** keyword. The **iphc-forma**t keyword indicates the type of header compression that will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, Rapid Transport Protocol (RTP) header-compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Because both TCP and RTP header compression are enabled, both TCP and UDP packets are compressed.

Note For Frame Relay interfaces, the **iphc-format** keyword is not available.

Header Compression ietf-format Keyword

This command includes the **ietf-format** keyword. The **ietf-format** keyword indicates the type of header compression that will be used. For HDLC interfaces, the **ietf-format** compresses only TCP packets. For PPP interfaces, when the **ietf-format** keyword is specified, RTP header-compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Because both TCP and RTP header compression are enabled, both TCP and UDP packets are compressed.

Note For Frame Relay interfaces, the **ietf-format** keyword is not available.

Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
```

The following example enables RTP header compression on the Serial1/0.0 subinterface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip tcp header-compression** command is specified:

```
Router(config)# interface serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
```

The following example enables RTP header compression on the Serial2/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified:

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

Related Commands

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

keepalive

To enable keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface, use the keepalive command in interface configuration mode. When the keepalive function is enabled, a **keepalive** packet is sent at the specified time interval to keep the interface active. To turn off keepalive packets entirely, use the no form of this command.

keepalive [*period***]**

no keepalive [*period*]

Syntax Description

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

Defaults

period: 10 seconds

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

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)MC2	This command was incorporated.
12.2(15)MC1	This command was incorporated.
12.3(11)T	This command was incorporated.

Usage Guidelines

Keepalive Time Interval

You can configure the keepalive time interval, which is the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (serial and tunnel), to ensure that a network interface is alive. The interval is adjustable in 1-second increments, down to a minimum of 1 second. An interface is declared down after three update intervals have passed without receiving a keepalive packet unless the retry value is set higher.

Setting the keepalive timer to a low value is very useful for rapidly detecting Ethernet interface failures (such as a transceiver cable disconnecting, or cable that is not terminated).

Line Failure

A typical serial line failure involves losing the Carrier Detect (CD) signal. Because this sort of failure is typically noticed within a few milliseconds, adjusting the keepalive timer for quicker routing recovery is generally not useful.

Keepalive Packets with Tunnel Interfaces

GRE keepalive packets may be sent either from both sides of a tunnel or from just one side. If they are sent from both sides, the period and retry parameters can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

Note When adjusting the keepalive timer for a very-low-bandwidth serial interface, large datagrams can delay the smaller keepalive packets long enough to cause the line protocol to go down. You may need to experiment to determine the best values to use for the timeout and the number of retry attempts.

Examples

The following example shows how to set the keepalive interval to 3 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)# keepalive 3
```

The following example shows how to set the keepalive interval to 3 seconds and the retry value to 7:

```
Router(config)# interface tunnel 1
Router(config-if)# keepalive 3 7
```

load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interva**l interface configuration command. Use the **no** form of this command to revert to the default setting.

load-interval *seconds*

no load-interval *seconds*

Syntax Description

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

Defaults

300 seconds (or 5 minutes)

Command Modes

Interface configuration

Command History

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

Usage Guidelines

If you want load computations to be more reactive to short bursts of traffic, rather than averaged over 5-minute periods, you can shorten the length of time over which load averages are computed.

If the load interval is set to 30 seconds, new data is used for load calculations over a 30-second period. This data is used to compute load statistics, including input rate in bits and packets per second, output rate in bits and packets per second, load, and reliability.

Load data is gathered every 5 seconds. This data is used for a weighted average calculation in which more-recent load data has more weight in the computation than older load data. If the load interval is set to 30 seconds, the average is computed for the last 30 seconds of load data.

The **load-interval** command allows you to change the default interval of 5 minutes to a shorter or longer period of time. if you change it to a shorter period of time, the input and output statistics that are displayed when you use the **show interface** command will be more current, and based on more instantaneous data, rather than reflecting a more average load over a longer period of time.

This command is often used for dial backup purposes, to increase or decrease the likelihood of a backup interface being implemented, but it can be used on any interface.

Examples

In the following example, the default 5-minute average is set to a 30-second average. A burst in traffic that would not trigger a dial backup for an interface configured with the default 5-minute interval might trigger a dial backup for this interface that is set for a shorter, 30-second interval.

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

Related Commands

Command	Description
show interfaces	Displays ALC information.

max-reserved-bandwidth

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

max-reserved-bandwidth *percent*

no max-reserved-bandwidth

Syntax Description

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

Defaults

The default percentage is 75 percent.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

match ip dscp

To identify a specific IP differentiated service code point (DSCP) value as a match criterion, use the **match ip dscp** class-map configuration command. To remove a specific IP DSCP value from a class map, use the **no** form of this command.

match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

no match ip dscp *ip-dscp-value* [*ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value*]

Syntax Description

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

Defaults

This command has no default behavior or values.

Command Modes

Class-map configuration

Command History

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

Usage Guidelines

Up to eight IP DSCP values can be matched in one match statement. For example, if you wanted the IP DSCP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values), enter the **match ip dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific IP DSCP value marking on a packet. The *ip-dscp-value* arguments are used as markings only. The IP DSCP values have no mathematical significance. For instance, the *ip-dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *ip-dscp-value* of 2 is different than a packet marked with the *ip-dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Examples

The following example shows how to configure the service policy called priority50 and attach service policy priority50 to an interface. In this example, the class map called ipdscp15 will evaluate all packets entering interface Fast Ethernet 1/0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet will be treated with a priority level of 55.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config-cmap)# exit
```

```
Router(config)# policy-map priority55
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority55
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fal/0/0
Router(config-if)# service-policy input priority55
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip dscp	Marks the IP DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

pos-scrambling

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

pos-scrambling

no pos-scrambling

Syntax Description

This command has no arguments or keywords.

Defaults

Scrambling is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

The following example enables scrambling on all POS interfaces.

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

The following example disables scrambling on all POS interfaces.

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

Related Commands

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

ppp multilink interleave

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

ppp multilink interleave

no ppp multilink interleave

SyntaxDescription This command has no arguments or keywords.

Command Modes Interface configuration

Command History

Release	Modification
11.3	This command is introduced.

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

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

ran-opt atm scrambling stream

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

ran-opt atm scrambling stream

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows scrambling-payload on ATM configuration:

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

show gsm traffic

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

show gsm traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show gsm traffic

GSM-Abis(Serial1/2:0): traffic (1sec/5sec/1min/5min/1hr) units(bps)
    compression traffic(  964000/  966758/  965928/  965937/  48831)
  decompression traffic(  132000/  136774/  134428/  134430/   6799)
```

show gsm-abis efficiency

To display history of the GSM compression/decompression efficiency averages at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals, use the **show gsm-abis efficiency** command in privileged EXEC mode. Efficiency is defined as the percentage of bandwidth savings obtained by using the compression/decompression algorithm to suppress GSM data.

show gsm-abis efficiency [history]

Syntax Description

history	Creates a graph display of the efficiency.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

Router# sh gsm eff history ser0/2:0

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


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

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

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



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


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


    999999999999999999999999999999999999999999999999999999
    111111111111111111111111111111111111111111111111111111
100
 90 ************************************************************
 80 ************************************************************
 70 ************************************************************
 60 ************************************************************
 50 ************************************************************
 40 ************************************************************
 30 ************************************************************
 20 ************************************************************
 10 ************************************************************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
 GSM-Abis(Serial0/2:0) decompression efficiency%/sec (last 60 secs)

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

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis errors

To display error statistics counters of the GSM compression/decompression, use the **show gsm-abis errors** command in privileged EXEC mode.

show gsm-abis errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show gsm-abis errors
GSM-Abis(Serial0/2:0): backhaul_rxLostPakInd =========== 1/431956
GSM-Abis(Serial0/2:0): backhaul_txLostPakInd =========== 1/432539
GSM-Abis(Serial0/2:0): backhaul_missedPaks ============= 654/431956
GSM-Abis(Serial0/2:0): backhaul_latePaks =============== 591
GSM-Abis(Serial0/2:0): backhaul_lostPaks =============== 1
GSM-Abis(Serial0/2:0): backhaul_txRset ================= 33
GSM-Abis(Serial0/2:0): backhaul_overun ================= 29
GSM-Abis(Serial0/2:0): compression_failures ============ 39661
GSM-Abis(Serial0/2:0): backhaul_congestion_drops ======= 39661
GSM-Abis(Serial0/2:0): backhaul_congestion_events ====== 1
GSM-Abis(Serial0/2:0): backhaul_congestion_duration(sec) == 80
GSM-Abis(Serial0/2:0): backhaul_congestion_bytes ========== 16498976
Last cleared 00:14:24
```

Table A-2 describes the significant fields shown in the display.

Table A-1 show gsm-abis errors Field Descriptions

Field	Description
tx_gsmPak_failures	Send GSM-Abis packer failed.
txPtcl_no_memory	No particles available, for example, getparticle() failure.
backhaul_peer_not_ready	Backhaul peer not ready for input.
backhaul_peer_not_active	Backhaul peer is not active. Backhaul peer is marked active when first. Backhaul peer is received from peer.
backhaul_invalid_pak	Received backhaulPak is invalid. Returns errCode to indentify reason.

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

Field	Description
backhaul_rxLostPakInd	Receive backhaul_lostPak indicator
backhaul_txLostPakInd	Transmit backhaul_lostPak indicator
backhaul_missedPak	Received backhaulPak is missed/dropped.
backhaul_latePaks	No backhaul packet arrived in time to fill txParticles with data (backhaul packet was lost or late).
backhaul_lostPaks	Backhaul packet was lost.
backhaul_txPtcl_no_memory	No particles available, for example, getparticle () failure.
backhaul_txReset	Packets lost due to txBufferRing reset.
decompression_failures	Decompression of input backhaulPak failed.
compression_failures	Compression of input GSM packet failed.
no-backhaul_pak_available	No memory for backhaulPak buffer.
no-backhaul_interface	Could not find an output interface that corresponds to configured remote ipAddr.
backhaul_interface_down	Interface used for backhaul is not active.
backhaul_encap_failures	The pak-encap failed.
backhaul_qos_classify_drops	QoS classification drops.
rxInterrupt_failures	Count number of Abis packets missed because of unexpected rxInterrupt.
abis_late	GSM-Abis rxInterrupt arrived too late.
abis_early	GSM-Abis rxInterrupt arrived too early.

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis packets

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

show gsm-abis packets

show gsm-abis packets | include retransmit

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show gsm-abis packets
GSM-Abis(Serial0/2:0): packets:
  rxGSM_count ================== 164011
  txGSM_count ================= 164011
  rxBackhaul_packets ========== 163428
  txBackhaul_packets ========== 164011
  rxBackhaul_bytes ============ 7649833
  txBackhaul_bytes ============ 7638262
  rx_sampleCount ============== 40674728
    rx_suppressedCount ======== 36629047
    rx_retransmittedCount ===== 0
    rx_all_presentCount ======= 29
  tx_sampleCount ============== 4053144
    tx_presentCount ========== 66522
    tx_all_presentCount ======= 8
  backhaul_forced_inclusions == 1
  Last cleared 00:05:27
```

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

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis peering

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

show gsm-abis peering [details]

Syntax Description

details	Provides detail information about peering.

Command Modes

Privileged EXEC

Command History

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

Examples

The following are examples outputs generated by this command.

```
Router# show gsm-abis peering ser0/2:0
GSM-Abis(Serial0/2:0): Peering Information
GSM-Abis(Serial0/2:0):  Local (10.10.10.1:5555) States:
GSM-Abis(Serial0/2:0):    Connect State Is:    CONNECTED
GSM-Abis(Serial0/2:0):    Local Alarm Is:      CLEAR (NO ALARM)
GSM-Abis(Serial0/2:0):    Redundancy State:    ACTIVE
GSM-Abis(Serial0/2:0):    Local Peer Version:  1.0
GSM-Abis(Serial0/2:0):  Remote (10.10.10.2:5555) States:
GSM-Abis(Serial0/2:0):    Remote Alarm Is:     CLEAR (NO ALARM)
GSM-Abis(Serial0/2:0):    Remote Peer Version: 1.0

Router# show gsm-abis peering detail ser0/2:0
GSM-Abis(Serial0/2:0): Peering Information (Version 1.0) History with current state at the
bottom GSM Peering History:

      Connect State Is:                                    System Time
      ------------------                                   -------------------
      DISCONNECT  *Apr 26 19:00:20.303
      SND_CONNECT                                          *Apr 26 15:48:30.568
      ACK_CONNECT                                        *Apr 26 15:48:31.572
    **CONNECTED                                            *Apr 26 15:50:57.113

      Local Peer Is:          Conn Info                    System Time
      ---------------------- ----------                    -------------------
      CLEAR (NO ALARM)        DISCONNECT                 *Mar 1 19:00:20.303
      SENDING AIS           DISCONNECT                     *Apr 24 15:48:31.980
    **CLEAR (NO ALARM)        CONNECTED                  *Apr 26 15:51:04.113

      Remote Peer Is:         Conn Info   Local Redundancy System Time
      ---------------------- ----------  ---------------- -------------------
      UNAVAILABLE             DISCONNECT  STANDBV  *Mar 1 19:00:20.303
      UNAVAILABLE           DISCONNECTACTIVE  *Mar 1 15:50:57.113
      RX LOF RED) ALARM  CONNECTED  ACTIVE  *Apr 26 15:50:57.117
    **CLEAR (NO ALARM)        CONNECTED ACTIVE  *Apr 26 15:50:57.117

Current System Time:                                     *Apr 26 16:00:33.133 est
```

```
 Peer Pak Info:
  No Backhaul Interface ======= 0 packets
  Backhaul Encap Failures ===== 0 packets
  Get CtrlPak Failures ======== 0 packets
  RX Ctrl Paks ================ 7 packets
  TX Ctrl Paks ================ 11 packets
  Out Of Sequence Paks ======== 1 packets
    Out Of Sequence Paks ====== 0 packets
  Unsolicited Connect Paks ==== 1 (times)
    Unsolicited Connect Paks == 0 (times)
  Remove Retransmit Errors ==== 8 (error)
  Backhaul QOS classify drops = 0 packets

 Peer Ctrl Type Info:
  Unknown Ctrl Types ========== 0 (times)
  Invalid Ctrl Lens =========== 0 (times)
  Missed Keepalives =========== 0 (times)
  Extra Keepalives ============ 0 (times)
  Peer Restarts =============== 5 (times)
    Due to Cfg Change ========= 2(times)
    Due to Internal Err ======= 1(times)
    Due to Lost Keepalive ===== 0 (times)
    Due to Interface Down ===== 0 (times)
    Due to Critical Pak Lost == 0 (times)
    Due to Interface Cleanup == 0 (times)
    Due to Excess Seq No Err == 0 (times)

 Peer Ctrl Variable Info:
  peer_enable ================= 1 (on/off)
  peer_ready ================== 1 (on/off)
  connecting ================== 0 (on/off)
  detectAlmErr ================ 1 (on/off)

 Peer Queue/Memory Info:
  Retransmition Contexts Used = 1 (in use)
  Data Buffers Used =========== 0 (in use)
  Seq Num: tx_fsn/tx_bsn ====== 4/4
  Seq Num: rx_fsn/rx_bsn ====== 4/4
 Adjacent serial number: 'FTX1021A44Q'

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show ip rtp header-compression

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **detail** keyword is not available with the **show ip rtp header-compression** command on a Route Switch Processor (RSP). However, the **detail** keyword is available with the **show ip rtp header-compression** command on a Versatile Interface Processor (VIP). Enter the **show ip rtp header-compression type number detail** command on a VIP to retrieve detailed information about RTP header compression on a specific interface.

Examples

The following is sample output from the **show ip rtp header-compression** command:

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
 Interface Serial1:
  Rcvd: 0 total, 0 compressed, 0 errors
     0 dropped, 0 buffer copies, 0 buffer failures
  Sent: 430 total 429 compressed
     15122 bytes saved, 0 bytes sent
     0 efficiency improvement factor
  Connect: 16 rx slots, 16 tx slots, 0 long searches, 1 misses
     99% hit ratio, five minute miss rate 0 misses/sec, 0 max.
```

Table A-2 describes the significant fields shown in the display.

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

Field	Description
Interface Serial1	Type and number of interface.
Rcvd: total	Number of packets received on the interface.
compressed	Number of packets with compressed header.
errors	Number of errors.
dropped	Number of dropped packets.
buffer copies	Not applicable to the Cisco MWR 1941-DC-A router.
buffer failures	Not applicable to the Cisco MWR 1941-DC-A router.
Sent: total	Total number of packets sent.
compressed	Number of packets sent with compressed header.
bytes saved	Total savings in bytes as a result of compression.
bytes sent	Not applicable to the Cisco MWR 1941-DC-A router.
efficiency improvement factor	Efficiency achieved through compression.
Connect: rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
long searches	Not applicable to the Cisco MWR 1941-DC-A router.
misses	Number of new states that were created.
hit ratio	Number of times that existing states were revised.
five minute miss rate	Average miss rate.
max.	Maximum miss rate.
negative cache	Not applicable to the Cisco MWR 1941-DC-A router.

Related Commands

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

show umts traffic

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

show umts traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show umts traffic

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

show umts-iub congestion

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

show umts-iub congestion

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub efficiency

To display history of the UMTS interface efficiency averages at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals, use the **show umts-iub efficiency** command in privileged EXEC mode. Efficiency is defined as the percentage of bandwidth savings obtained by using the compression/decompression algorithm to suppress GSM data.

show umts-iub efficiency [history]

Syntax Description

history	Creates a graph display of the efficiency.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub errors

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

show umts-iub errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

Example 1:

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

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

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

Example 2

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

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

5 is also the number of packets.
```

Example 3

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

```
Router# show umts errors

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

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

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub packets

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

show umts-iub packets

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

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

show umts-iub peering

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

show umts-iub peering [details]

Syntax Description

details	Provides detail information about peering.

Command Modes

Privileged EXEC

Command History

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

Examples

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

Example 1

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

Example 2

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


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

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

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

Example 3 Brief report for all ATM interfaces

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

Example 4 with Alternate Backhaul (192.168.10.2 to 192.168.10.1)

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

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

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

Related Commands

Command	Description
clear umts-iub	Clears the statistics displayed.

show umts-iub pvc

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

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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



Local VCDs (not sent):

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

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

snmp-server enable traps ipran

To enable all ipran notifications via Simple Network Management Protocol (SNMP) notifications (traps) available on your system, use the **snmp-server enable traps ipran** command in global configuration mode. To disable ipran alarm-gsm notifications, use the **no** form of this command.

snmp-server enable traps ipran

no snmp-server enable traps ipran

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default. No notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)MR1	This command was introduced.

Examples

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

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

Related Commands

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

snmp-server enable traps ipran alarm-gsm

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

snmp-server enable traps ipran alarm-gsm

no snmp-server enable traps ipran alarm-gsm

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default. No notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)MR1	This command was introduced.

Examples

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

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

Related Commands

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

snmp-server enable traps ipran alarm-umts

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

snmp-server enable traps ipran alarm-umts

no snmp-server enable traps ipran alarm-umts

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default. No notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)MR1	This command was introduced.

Examples

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

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

Related Commands

Command	Description
snmp-server enable traps ipran alarm-gsm	Provides information alarms associated with GSM-Abis interfaces.
snmp-server enable traps ipran util	Provides information on backhaul utilization.
snmp-server enable traps ipran	Enables all notifications.

snmp-server enable traps ipran util

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

snmp-server enable traps ipran util

no snmp-server enable traps ipran util

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default. No notifications are sent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)MR1	This command was introduced.

Examples

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

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

Related Commands

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

umts local

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

umts local [ip-address]

Syntax Description

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

Command Modes

Sub-Interface configuration

Command History

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

Examples

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

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

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

Related Commands

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

umts remote

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

umts remote [ip-address]

Syntax Description

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

Command Modes

Sub-Interface configuration

Command History

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

Examples

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

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

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

Related Commands

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

umts-iub backhaul-oam

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

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

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

umts-iub backhaul-oam

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the local parameters:

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

umts-iub backhaul-mtu

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

umts-iub backhaul-mtu *byte-number*

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Examples

The following example sets the MTU value to 350 bytes:

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

umts-iub backhaul-timer

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

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

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

Syntax Description

This command has no arguments or keywords.

Defaults

Timer value of 1 ms.

Command Modes

Interface configuration

Command History

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

Examples

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

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

umts-iub congestion priority

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

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

Syntax Description

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

Defaults

The default setting is 9.

Command Modes

PVC configuration

Command History

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

Examples

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

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

Related Commands

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

umts-iub congestion-control

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

umts-iub congestion-control

Syntax Description

This command has no arguments or keywords.

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

umts-iub local

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

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

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the local parameters:

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

Related Commands

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

umts-iub remote

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

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

Syntax Description

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

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the remote parameters:

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

Related Commands

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

umts-iub set dscp

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

umts-iub set dscp *value*

Note Use this command when configuring UMTS shorthaul interfaces.

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the parameters:

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

Related Commands

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

umts-iub set dscp

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

umts-iub set dscp *value*

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

Syntax Description

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

Defaults

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

Command Modes

ATM-VC configuration

Command History

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

Examples

The following example shows how to configure the remote parameters:

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

Related Commands

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

umts-iub set peering dscp

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

umts-iub set peering dscp *value*

Note Use this command when configuring UMTS shorthaul interfaces.

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the parameters:

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

Related Commands

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