



APPENDIX **A**

Cisco 3825 Mobile Wireless Edge Router RAN-O Command Reference

This appendix contains an alphabetical listing of new and revised commands specific to the Cisco 3825 router in a Radio-Access Network-Optimization (RAN-O) solution.

The following commands have been introduced:

- [atm umts](#)
- [atm umts-iub](#)
- [cem-group](#)
- [class cem](#)
- [clear gsm-abis](#)
- [clear umts-iub](#)
- [de jitter-buffer](#)
- [gsm-abis congestion abate](#)
- [gsm-abis congestion critical](#)
- [gsm-abis congestion enable](#)
- [gsm-abis congestion onset](#)
- [gsm-abis jitter](#)
- [gsm-abis local](#)
- [gsm-abis remote](#)
- [gsm-abis retransmit](#)
- [gsm-abis set dscp](#)
- [idle-pattern](#)
- [pw-pvc](#)
- [sample-rate](#)
- [show cem circuit](#)
- [show cem platform](#)
- [show gsm-abis efficiency](#)
- [show gsm-abis errors](#)
- [show gsm-abis packets](#)

- `show gsm-abis peering`
- `show gsm-abis traffic`
- `show umts-iub congestion`
- `show umts-iub efficiency`
- `show umts-iub errors`
- `show umts-iub packets`
- `show umts-iub peering`
- `show umts-iub pvc`
- `show umts-iub traffic`
- `snmp-server enable traps ipran`
- `snmp-server enable traps ipran alarm-gsm`
- `snmp-server enable traps ipran alarm-umts`
- `snmp-server enable traps ipran util`
- `umts-iub backhaul-oam`
- `umts-iub backhaul-timer`
- `umts-iub congestion-control`
- `umts-iub congestion priority`
- `umts-iub local`
- `umts-iub remote`
- `umts-iub set dscp` (interface configuration mode)
- `umts-iub set dscp` (PVC configuration mode)
- `umts-iub set peering dscp`
- `umts local`
- `umts remote`

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

- `backup delay`
- `backup peer`
- `cdp enable`
- `clear ip rtp header-compression`
- `encapsulation l2tpv3`
- `ima-group`
- `interface atm ima`
- `ip local interface`
- `ip protocol`
- `ip rtp header-compression`
- `ip tcp header-compression`
- `ip tos (l2tp)`
- `ipran-mib backhaul-notify-interval`

- [ipran-mib location](#)
- [ipran-mib snmp-access](#)
- [ipran-mib threshold-acceptable](#)
- [ipran-mib threshold-overloaded](#)
- [ipran-mib threshold-warning](#)
- [keepalive](#)
- [load-interval](#)
- [match ip dscp](#)
- [mode y-cable](#)
- [mpls ip](#)
- [pseudowire-class](#)
- [redundancy](#)
- [scrambling-payload](#)
- [sequencing](#)
- [show atm cell-packing](#)
- [show connection](#)
- [show mpls l2transport vc](#)
- [show l2tp session](#)
- [show l2tp tunnel](#)
- [show ip rtp header-compression](#)
- [show redundancy](#)
- [show xconnect all](#)
- [standalone](#)
- [standby use-interface](#)
- [xconnect](#)
- [xconnect logging redundancy](#)

atm umts

To select an ATM interface for Universal Mobile Telecommunications System (UMTS) Iub traffic for the atm subinterfaces, use the **atm umts** Sub-Interface configuration command. This command is used when you want to off load one or more permanent virtual circuit (PVC) traffic packets from a physical ATM shorthaul so as to go over 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.

atm umts

Syntax Description

This command has no arguments or keywords.

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 **atm umts** command.

```
Router(config)# interface ATM0/2/0
Router(config-if)# atm umts-iub
Router(config-subif)# atm umts
```



Note

You can use this command only when the base atm interface is already enabled as **atm umts**.

Related Commands

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

atm umts-iub

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

atm umts-iub

Syntax Description	This command has no arguments or keywords.
---------------------------	--

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 atm umts command.
-----------------	---

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

backup delay

To specify how long a backup pseudowire (PW) virtual circuit (VC) should wait before resuming operation after the primary PW VC goes down, use the **backup delay** command in the interface configuration mode or xconnect configuration mode.

backup delay *enable-delay* [*disable-delay* | **never**]

Syntax Description

<i>enable-delay</i>	Number of seconds that elapse after the primary PW VC goes down before the Cisco IOS software activates the secondary PW VC. The range is 0 to 180. The default is 0.
<i>disable-delay</i>	Number of seconds that elapse after the primary PW VC comes up before the Cisco IOS software deactivates the secondary PW VC. The range is 0 to 180. The default is 0.
never	The secondary PW VC does not fall back to the primary PW VC if the primary PW VC becomes available again, unless the secondary PW VC fails.

Defaults

If a failover occurs, the xconnect redundancy algorithm immediately switches over or falls back to the backup or primary member in the redundancy group.

Command Modes

Interface configuration
Xconnect configuration

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(16)MR	This command was integrated into Cisco IOS Release 12.4(16)MR.

Examples

The following example shows a Multiprotocol Label Switching (MPLS) xconnect with one redundant peer. Once a switchover to the secondary VC occurs, there is no fallback to the primary VC unless the secondary VC fails.

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0/0
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 0 never
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

The following example shows an MPLS xconnect with one redundant peer. The switchover does not begin unless the Layer 2 Tunnel Protocol (L2TP) PW has been down for three seconds. After a switchover to the secondary VC occurs, there is no fallback to the primary until the primary VC has been reestablished and is up for ten seconds.

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0/0
Router(config-if)# xconnect 10.0.0.1 50 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 50
Router(config-if-xconn)# backup delay 3 10
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
backup peer	Configures a redundant peer for a PW VC.

backup peer

To specify a redundant peer for a PW VC, use the **backup peer** command in the interface configuration mode or xconnect configuration mode. To remove the redundant peer, use the **no** form of this command.

backup peer *peer-router-ip-addr* *vcid* [**pw-class** *pw-class-name*]

no backup peer *peer-router-ip-addr* *vcid*

Syntax Description

<i>peer-router-ip-addr</i>	IP address of the remote peer.
<i>vcid</i>	The 32-bit identifier of the VC between the routers at each end of the layer control channel.
pw-class	(Optional) PW type. If not specified, the PW type is inherited from the parent xconnect.
<i>pw-class-name</i>	(Optional) Name of the PW you created when you established the PW class.

Defaults

No redundant peer is established.

Command Modes

Interface configuration
Xconnect configuration

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(16)MR	This command was integrated into Cisco IOS Release 12.4(16)MR.

Usage Guidelines

The combination of the *peer-router-ip-addr* and *vcid* arguments must be unique on the router.

Examples

The following example shows an MPLS xconnect with one redundant peer:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm1/0/0
Router(config-if)# xconnect 10.0.0.1 100 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 200
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```


The following example shows a backup peer configuration for an ATM interface:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# exit
Router(config)# interface atm0/0/1
Router(config-if)# xconnect 10.0.0.2 1 pw-class mpls
Router(config-if-xconn)# backup peer 10.0.0.2 100 pw-class mpls
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
backup delay	Specifies how long the backup PW VC should wait before resuming operation after the primary PW VC goes down.

cdp enable

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

cdp enable

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

cem-group

To create a circuit emulation (CEM) channel from one or more time slots of a T1 or E1 line, use the **cem-group** command in controller configuration mode. To remove a CEM group and release the associated time slots, use the **no** form of this command.

cem-group *group-number* {**unframed** | **timeslots** *time-slot-range*}

no cem-group *group-number*

Syntax Description

<i>group-number</i>	CEM identifier to be used for this group of time slots: <ul style="list-style-type: none"> For T1 ports, the range is from 0 to 23. For E1 ports, the range is from 0 to 30.
unframed	Specifies that a single CEM channel is being created, including all time slots, without specifying the framing structure of the line.
timeslots	Specifies that a list of time slots is to be used as specified by the <i>time-slot-range</i> argument. <i>time-slot-range</i> —Specifies the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.

Defaults

No CEM groups are defined.

Command Modes

Controller configuration

Command History

Release	Modification
12.4(12)MR2	This command was introduced.

Usage Guidelines

Use this command to create CEM channels on the T1 or E1 port.

Examples

The following example illustrates the use of the **cem group** command:

SATOP

```
Router# config t
Router(config)# controller el 0/0/0
Router(config-controller)# cem-group 0 unframed
Router(config-controller)# exit
Router(config)# interface cem 0/0/0
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
```

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

CESoPSN

```
Router# config t
Router(config)# controller el 0/0/1
Router(config-controller)# cem-group 0 timeslots 1-31
Router(config-controller)# exit
Router(config)# interface cem 0/0/1
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	cem	Enters circuit emulation configuration mode.

class cem

Use the **class cem** command in the global configuration mode to configure CEM interface parameters in a class that's applied to CEM interfaces together. This command works in the same manner for CEM interfaces as pseudowire-class does for xconnect.

class cem *class-name*

Syntax Description	<i>class-name</i> (Required) The name of a CEM interface parameters class.						
Command Modes	Global configuration						
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.4(12)MR2</td><td>This command was introduced.</td></tr> </table>	Release	Modification	12.4(12)MR2	This command was introduced.		
Release	Modification						
12.4(12)MR2	This command was introduced.						
Usage Guidelines	<p>The class cem command allows you to configure CEM interface parameters in a class that's applied to CEM interfaces together. A class cem command includes the following configuration settings:</p> <ul style="list-style-type: none"> de jitter-buffer <i>de jitter in ms</i> idle-pattern <i>Set 8 bit idle pattern</i> sample-rate <i>Sample rate (in ms)</i> 						
Examples	<p>The following example illustrates the use of the class cem command:</p> <pre>Router# config t Router(config)# class cem mycemclass Router(config-cem-class)# de jitter-buffer 10 Router(config-cem-class)# sample-rate 2 Router(config-cem-class)# exit Router(config)# interface cem 0/0/0 Router(config-if)# no ip address Router(config-if)# cem 0 Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls Router(config-if-cem-xconn)# cem class mycemclass Router(config-if-cem)# exit Router(config-if)# exit Router(config)# exit</pre>						
Related Commands	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td>de jitter-buffer</td><td>Specifies the size of the de jitter-buffer used for the network jitter in the CEM configuration mode.</td></tr> <tr> <td>idle-pattern</td><td>Specifies the data pattern to transmit on the T1/E1 when missing packets are detected on the PWE3 circuit in the CEM configuration mode.</td></tr> </table>	Command	Description	de jitter-buffer	Specifies the size of the de jitter-buffer used for the network jitter in the CEM configuration mode.	idle-pattern	Specifies the data pattern to transmit on the T1/E1 when missing packets are detected on the PWE3 circuit in the CEM configuration mode.
Command	Description						
de jitter-buffer	Specifies the size of the de jitter-buffer used for the network jitter in the CEM configuration mode.						
idle-pattern	Specifies the data pattern to transmit on the T1/E1 when missing packets are detected on the PWE3 circuit in the CEM configuration mode.						

Command	Description
sample-rate	Specifies in milliseconds the rate hardware samples the data on the attached circuit in the CEM circuit configuration mode.
cem	Enters circuit emulation configuration mode.

clear gsm-abis

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

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

Syntax Description

serial	
<i>serial-number</i>	(Optional) The serial number range is from 0 to6.
<i>interface number</i>	(Optional) The serial number range is from 0 to6.

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 serial option.

Examples

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

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

Related Commands

Command	Description
show gsm-abis efficiency	Displays the history of Global System for Mobile Communications (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.

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
11.3	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.
12.4(2)MR	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** *atm interface interface number*]

Syntax Description

atm

atm interface

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

interface number

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

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 0/0/1**

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.

de jitter-buffer

To specify the size of the de jitter-buffer used to compensate for the network jitter, use the **de jitter-buffer** command in the CEM configuration mode. To restore the de jitter-buffer to its default size, use the **no** form of this command.

de jitter-buffer *size*

no de jitter-buffer

Syntax Description

<i>size</i>	Use the <i>size</i> argument to specify the size of the buffer in milliseconds. <i>Size</i> can vary from 4 to 500 ms; default is 4 ms.
-------------	---

Defaults

The de jitter buffer defaults to 4 milliseconds.

Command Modes

CEM circuit configuration

Command History

Release	Modification
12.4(12)MR2	This command was introduced.

Examples

The following example illustrates the use of the **de jitter-buffer** command:

```
Router# config t
Router(config)# interface cem 0/0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# de jitter-buffer 10
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
cem class	Applies the CEM interface parameters defined in the given <cem-class-name> to the circuit.
class cem	Configure's CEM interface parameters in a class that's applied to CEM interfaces together in the global configuration mode.

encapsulation l2tpv3

To specify that Layer 2 Tunnel Protocol version 3 (L2TPv3) is used as the data encapsulation method for tunneling IP traffic over the PW, use the **encapsulation l2tpv3** command in pseudowire-class configuration mode. To remove L2TPv3 as the encapsulation method, use the **no pseudowire-class** command (see the Usage Guidelines for more information).

encapsulation l2tpv3

no pseudowire-class

Syntax Description This command has no arguments or keywords.

Defaults No encapsulation method is specified.

Command Modes Pseudowire-class configuration

Command History	Release	Modification
	12.0(23)S	This command was introduced.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines This command must be configured if the pseudowire-class is referenced from an xconnect configured to forward L2TPv3 traffic.

Once you specify the **encapsulation l2tpv3** command, you cannot remove it using the **no encapsulation l2tpv3** command. Nor can you change the command's setting using the **encapsulation mpls** command. Those methods result in the following error message:

```
Encapsulation changes are not allowed on an existing pw-class.
```

To remove the **l2tpv3** command, you must delete the PW with the **no pseudowire-class** command. To change the type of encapsulation, remove the PW with the **no pseudowire-class** command to re-establish the PW and to specify the new encapsulation type.

Examples The following example illustrates the use of the **encapsulation l2tpv3** command:

```
Router# config t
Router(config)# pseudowire-class l2tp
Router(config-pw-class)# encapsulation l2tpv3
Router(config-pw-class)# exit
Router(config)# exit
```

The following example configures ATM AAL5 over L2TPv3 PW:

```
Router# config t
Router(config)# interface atm 0/0/1
Router(config-if)# pvc 0/10 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aal5
Router(config-if-atm-l2trans-pvc)# xconnect 1.1.1.1 10 pw-class l2tp
Router(config-if-atm-l2trans-pvc-xconn)# exit
Router(config-if-atm-l2trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
encapsulation mpls	Configures MPLS as the data encapsulation method over AToM-enabled IP/MPLS networks.
pseudowire-class	Specifies the name of an L2TP pseudowire-class and enters pseudowire-class configuration mode.

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 Serial10/1/0:0
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 Internet Protocol/User Datagram Protocol (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 Base Transceiver Station (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 Serial10/1/0:0
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.

■ **gsm-abis congestion critical**

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 Serial10/1/0:0
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 Serial10/1/0:0
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	<i>ms</i> 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 Serial10/1/0:0
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 Datagram 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.
<i>port</i>	(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 Serial10/1/0.0
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 Datagram 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.
<i>port</i>	(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 Serial10/1/0.0
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	<i>sample-delay</i>	The number of duplicate samples that must be observed before the duplicate sample will be retransmitted. The <i>sample-delay</i> 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 Serial10/1/0.0
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

<i>value</i>	A number from 0 to 63 or hex value that sets the GSM-Abis DSCP value.
--------------	---

Defaults

There are no default settings or behaviors.

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 Serial10/1/0.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis local 10.10.10.1 5504
Router(config-if)# gsm-abis remote 10.10.10.2 5504
Router(config-if)# gsm-abis set dscp cs2
```

idle-pattern

To specify the data pattern transmitted on the T1/E1 when missing packets are detected on the PWE3 circuit, use the **idle-pattern** command in CEM configuration mode.

idle-pattern [*pattern*]

no idle-pattern

Syntax Description	<i>pattern</i>	An 8-bit hexadecimal number that is transmitted as the idle pattern.
--------------------	----------------	--

Defaults	Default idle-pattern is 0xFF.
----------	-------------------------------

Command Modes	CEM circuit configuration
---------------	---------------------------

Command History	Release	Modification
	12.4(12)MR2	This command was introduced.

Usage Guidelines	The idle-pattern data is sent to replace the data from missing packets.
------------------	---

Examples	The following example illustrates the use of the idle-pattern command:
----------	---

```
Router# config t
Router(config)# interface cem 0/0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# idle-pattern 0x55
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	cem	Enters circuit emulation configuration mode.
	cem class	Applies the CEM interface parameters defined in the given <cem-class-name> to the circuit.
	class cem	Configure's CEM interface parameters in a class that's applied to CEM interfaces together in the global configuration mode.

ima-group

To define physical links as inverse multiplexing over ATM (IMA) group members, use the **ima-group** Interface configuration command. When you first perform the configuration or when you change the group number, the interface is automatically disabled, moved to the new group, and then enabled. To remove the port from the group, use the **no** form of this command.

ima-group *group-number*

Syntax Description

<i>group-number</i>	Specifies an IMA group number from 0 to 3. IMA groups can span multiple ports on a port adapter but cannot span port adapters.
---------------------	--

Defaults

Physical links are not included in IMA groups.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced.
12.4(4)MR	This command was incorporated.

Usage Guidelines

Use the **ima-group** interface command to configure a T1/E1 IMA port adapter interface as part of an IMA group.

Examples

The following example shows how to define an IMA group:

```
Router(config)# interface ATM0/0/0
Router(config-if)# no ip address
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# ima-group 0
```

Related Commands

Command	Description
interface atm	Configures an ATM interface.
interface atm ima	Configures an ATM IMA group.
show ima interface atm	Provides information about configured IMA groups or a specific IMA group.

interface atm ima

To configure an ATM IMA group and enter interface configurations mode, use the **interface atm ima** global configuration command. If the group does not exist when the command is issued, the command automatically creates the group.

interface atm *slot/ima*<group-number>

Syntax Description	slot	Specifies the slot location of the ATM IMA port adapter.
	group-number	Specifies an IMA group number from 0 to 3. You can create up to four groups.

Defaults By default there are no IMA groups, only individual ATM links.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)XE	This command was introduced.
	12.4(4)MR	This command was incorporated.

Usage Guidelines When a port is configured for IMA functionality, it no longer operates as an individual ATM link. Specifying ATM links as members of a group using the ima-group interface command does not enable the group. You must use the **interface atm slot/ima**<group-number> command to create the group.

Examples The following example shows the how to create the IMA group:

```
Router(config)# interface ATM0/IMA0
Router(config-if)# no ip address
```

Related Commands	Command	Description
	ima-group	Configures the physical links as IMA group members; execute this interface configuration command for each physical link that you include in an IMA group.
	ima group-id	Enables the user to configure the IMA Group ID for the IMA interface.
	interface atm	Configures physical links for ATM.
	show ima interface atm	Displays general and detailed information about IMA groups and the links they include.

ip local interface

To configure the IP address of the provider edge (PE) router interface to be used as the source IP address for sending tunneled packets, use the **ip local interface** command in the pseudowire-class configuration mode. To remove the IP address, use the **no** form of this command.

ip local interface *interface-name*

no ip local interface *interface-name*

Syntax Description

<i>interface-name</i>	Name of the PE interface whose IP address is used as the source IP address for sending tunneled packets over a Layer 2 PW.
-----------------------	--

Defaults

No IP address is configured.

Command Modes

Pseudowire-class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines

Use the same local interface name for all pseudowire-classes configured between a pair of PE routers. It is highly recommended that you configure a loopback interface with this command. If you do not, the router chooses the “best available local address,” which could be any IP address configured on a core-facing interface. This configuration could prevent a control channel from being established.



Note

This command must be configured for pseudowire-class configurations using L2TPv3 as the data encapsulation method.

Examples

The following example shows how to configure the IP address of the local loopback 0 as the source IP address for sending packets through an L2TPv3 session:

```
Router# config t
Router(config)# pseudowire-class l2tp
Router(config-pw-class)# ip local interface loopback 0
Router(config-pw-class)# exit
Router(config)# exit
```

Related Commands	Command	Description
	ima-group	Configures the physical links as IMA group members, which executes the interface configuration command for each physical link included in an IMA group.
	ima group-id	Enables the user to configure the IMA Group ID for the IMA interface.
	interface atm	Configures physical links for ATM.
	show ima interface atm	Displays general and detailed information about IMA groups and the links they include.

ip protocol

To configure the Layer 2 Tunnel Protocol (L2TP) or Universal Tunnel Interface (UTI) as the IP protocol used for tunneling packets in a Layer 2 PW, use the **ip protocol** command in the pseudowire-class configuration mode. To remove the IP protocol configuration, use the **no** form of this command.

ip protocol {l2tp | uti | udp}

no ip protocol {l2tp | uti | udp}

Syntax Description

l2tp	(Default) Configures L2TP as the IP protocol used to tunnel packets in a Layer 2 PW.
uti	Configures UTI as the IP protocol used to tunnel packets in a Layer 2 PW and allows a router running L2TPv3 to interoperate with a peer running UTI.
udp	Configures UDP as the IP protocol used to tunnel packets in a Layer 2 PW.

Defaults

The default IP protocol is L2TP.

Command Modes

Pseudowire-class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines

The **ip protocol uti** command is not supported on the Cisco 3825 router. You can use the **ip protocol** command only if you have already entered the **encapsulation l2tpv3** command.

Examples

The following example shows how to configure l2tp as the IP protocol used to tunnel packets in an L2TPv3 PW created from the pseudowire-class named "l2tp":

```
Router# config t
Router(config)# pseudowire-class l2tp
Router(config-pw-class)# encapsulation l2tpv3
Router(config-pw-class)# ip protocol l2tp
Router(config-pw-class)# exit
Router(config)# exit
```

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire-class and enters pseudowire-class configuration mode.

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.
12.4(2)MR	This command was incorporated.

Usage Guidelines

You can compress IP/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 Serial1/0/0 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 Serial1/0/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# exit
```

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

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 20
Router(config-if)# exit
```

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

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0/0
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 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-format** 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 Serial1/0/0.0 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 serial1/0/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
```

The following example enables RTP header compression on the Serial1/0/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified:

```
Router(config)# interface serial1/0/0.0
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.

ip tos (l2tp)

To configure the Type of Service (ToS) byte in the header of Layer 2 tunneled packets, use the **ip tos** command in the pseudowire-class configuration mode. To disable a configured ToS value or IP ToS reflection, use the **no** form of this command.

ip tos { *value value* | **reflect** }

no tos { *value value* | **reflect** }

Syntax Description

value <i>value</i>	Sets the value of the ToS byte for IP packets in a L2TPv3 session. Valid values range from 0 to 255. The default value is 0.
reflect	Sets the value of the ToS byte for IP packets in an L2TPv3 session to be reflected from the inner IP header.

Defaults

The default ToS value is 0.

Command Modes

Pseudowire-class configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines

The **ip tos** command allows you to manually configure the value of the ToS byte used in the headers of Layer 2 tunneled packets or to have the ToS value reflected from the IP header of the encapsulated packet.



Note

IP ToS byte reflection functions only if traffic in an L2TPv3 session carries IP packets as its payload.

In addition, you can configure both IP ToS reflection and a ToS priority level (from 0 to 255) for a pseudowire-class. In this case, the ToS value in the tunnel header defaults to the value you specify with the **ip tos value** *value* command. IP packets received on the Layer 2 interface and encapsulated into the L2TPv3 session have their ToS byte reflected into the outer IP session, overriding the default value configured with the **ip tos value** *value* command.

Examples

In the following example, the ToS byte in the headers of tunneled packets in Layer 2 tunnels created from the pseudowire-class named “l2tp” is set as 5:

```
Router# config t
Router(config)# pseudowire-class l2tp
Router(config-pw-class)# ip tos 5
```

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

Related Commands

Command	Description
pseudowire-class	Specifies the name of an L2TP pseudowire-class and enters pseudowire-class configuration mode.

ipran-mib backhaul-notify-interval

Use the **ipran-mib backhaul-notify-interval** command in the global configuration mode to specify the interval used to suppress the generation of the ciscoIpRanBackHaulRcvdUtil and the ciscoIpRanBackHaulSentUtil notifications from the CISCO-IP-RAN-BACKHAUL-MIB.

To set the interval used to suppress notifications, use the following configuration command or the **no** form of this command to remove the interval:

ipran-mib backhaul-notify-interval *60-900 seconds*

Notifications are suppressed for the number of seconds specified. Notifications are not suppressed when this keyword is set to zero. The minimum interval is one minute and the maximum is fifteen minutes. When suppression is enabled, notifications are generated when a worse state is encountered. For example, the following transitions generate notifications:

- “acceptable” to “warning”
- “warning” to “overloaded”

Later transitions to lesser states are suppressed. For example, the following transitions do not generate notifications:

- “warning” to “acceptable”
- “overloaded” to “warning”
- “overloaded” to “acceptable”

At the end of the specified interval, a notification is generated if the current state is different from the state reported by the last notification.

Syntax Description

ipran-mib backhaul-notify-interval	60-900 seconds
---	----------------

Defaults

Defaults to 0 (notifications are not suppressed).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR1	This command was introduced.
12.4(9)MR	Support for utilization notification was removed. This command is supported to maintain compatibility.

Examples

```
Router# conf t
Router(config)# ipran-mib backhaul-notify-interval 60
Router(config)# ipran-mib backhaul-notify-interval 900
Router(config)# no ipran-mib backhaul-notify-interval
Router(config)# exit
```

Related Commands

Command	Description
ipran-mib threshold-acceptable	Specifies the acceptable level of traffic.
ipran-mib threshold-overloaded	Specifies the amount of traffic that indicates the backhaul is overloaded.
ipran-mib threshold-warning	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.

ipran-mib location

Use the **ipran-mib location** command in the global configuration mode to define the location of the device. It is also used to assist the network management system in properly displaying the topology of the system.

ipran-mib location *location*

Syntax Description	ipran-mib location ? <ul style="list-style-type: none"> addSite located at BSC or RNC site. cellSite Located at BTS or Node B site. undefined Undefined location. 	
Defaults	cellSite.	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.4(2)MR1	This command was introduced.
	12.4(9)MR	Support for utilization notification was removed. This command is supported to maintain compatibility.
Examples	<pre> Router# config t Router(config)# ipran-mib location aggSite Router(config)# ipran-mib location cellSite Router(config)# ipran-mib location undefined Router(config)# no ipran-mib location Router(config)# exit </pre>	
Related Commands	Command	Description
	ipran-mib snmp-access	Defines the type of connectivity between the device and the network management system.

ipran-mib snmp-access

Use the **ipran-mib snmp-access** command in the global configuration mode to define the type of connectivity between the device and the network management system. It is used to limit the amount of traffic when in band polling.

ipran-mib snmp-access *access*

Syntax Description

ipran-mib snmp-access ?

- inBand In Band SNMP connectivity.
- outOfBand Out of Band SNMP.
- undefined Undefined connectivity.

Defaults

inBand.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(2)MR1	This command was introduced.
12.4(9)MR	Support for utilization notification was removed. This command is supported to maintain compatibility.

Examples

```
Router# config t
Router(config)# ipran-mib snmp-access inBand
Router(config)# ipran-mib snmp-access outOfBand
Router(config)# ipran-mib snmp-access undefined
Router(config)# no ipran-mib snmp-access
Router(config)# exit
```

Related Commands

Command	Description
ipran-mib location	Defines the location of the device. It is also used to assist the network management system in properly displaying the topology of the system.

ipran-mib threshold-acceptable

Use the **ipran-mib threshold-acceptable** command in the global configuration mode to specify a level of traffic below which the instances of the cirbhBackHaulRcvdUtilState and cirbhBackHaulSentUtilState objects are marked as “acceptable.” All changes to this threshold takes affect at the end of the current interval. The value for this object must be less than the values specified by **ipran-mib threshold-warning** and **ipran-mib threshold-overloaded** command keywords. This parameter corresponds to the cirbhBackHaulAcceptableThreshold object.

ipran-mib threshold-acceptable [20-100 Utilization (percent)]

Syntax Description	ipran-mib threshold-acceptable ipran-mib threshold-acceptable percent.
---------------------------	---

Defaults	60 percent.
-----------------	-------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.4(2)MR1	This command was introduced.
	12.4(9)MR	Support for utilization notification was removed. This command is supported to maintain compatibility.

Examples	<pre>Router# config t Router(config)# ipran-mib threshold-acceptable 50 Router(config)# ipran-mib threshold-acceptable 70 Router(config)# no ipran-mib threshold-acceptable Router(config)# exit</pre>
-----------------	--

Related Commands	Command	Description
	ipran-mib threshold-overloaded	Specifies the amount of traffic that indicates the backhaul is overloaded.
	ipran-mib threshold-warning	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.
	ipran-mib backhaul-notify-interval	Specifies the interval used to suppress the generation of utilization notifications.

ipran-mib threshold-overloaded

Use the **ipran-mib threshold-overloaded** command in the global configuration mode to specify a level of traffic where the instances of the cirbhBackHaulRcvdUtilState and cirbhBackHaulSentUtilState objects are marked as “overloaded.” Changes to this threshold take affect at the end of the current interval. The value for this object must be greater than the value specified for the cirbhBackHaulAcceptableThreshold object. Also, the value for this object must be greater than or equal to value of the cirbhBackHaulWarningThreshold object.

ipran-mib threshold-overloaded [40-100 Utilization default (percent)]

Syntax Description	ipran-mib threshold-overload	ipran-mib threshold-overload percent
--------------------	------------------------------	--------------------------------------

Defaults	80 percent.
----------	-------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.4(2)MR1	This command was introduced.
	12.4(9)MR	Support for utilization notification was removed. This command is supported to maintain compatibility.

Examples

```
Router# config t
Router(config)# ipran-mib threshold-overloaded 60
Router(config)# ipran-mib threshold-overloaded 80
Router(config)# no ipran-mib threshold-warning
Router(config)# exit
```

Related Commands	Command	Description
	ipran-mib threshold-acceptable	Specifies the acceptable level of traffic.
	ipran-mib backhaul-notify-interval	Specifies the interval used to suppress the generation of utilization notifications.
	ipran-mib threshold-warning	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.

ipran-mib threshold-warning

Use the **ipran-mib threshold-warning** command in the global configuration mode to specify a level of traffic where the instances of the cirbhBackHaulRcvdUtilState and cirbhBackHaulSentUtilState objects are marked as “warning.”

All changes to this threshold take affect at the end of the current interval. The value for this object must be greater than the value specified for the **ipran-mib threshold-acceptable** command keyword.

Also, the value for this object must be less than or equal to value of the cirbhBackHaulOverloadedThreshold object. This parameter corresponds to the cirbhBackHaulWarningThreshold object.

ipran-mib threshold-warning [30-100 Utilization default (percent)]

Syntax Description	ipran-mib threshold-warning	ipran-mib threshold-warning percent
---------------------------	------------------------------------	-------------------------------------

Defaults	70 percent.
-----------------	-------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.4(2)MR1	This command was introduced.
	12.4(9)MR	Support for utilization notification was removed. This command is supported to maintain compatibility.

Examples	<pre>Router# config t Router(config)# ipran-mib threshold-warning 60 Router(config)# ipran-mib threshold-warning 80 Router(config)# no ipran-mib threshold-warning Router(config)# exit</pre>
-----------------	---

Related Commands	Command	Description
	ipran-mib threshold-acceptable	Specifies the acceptable level of traffic.
	ipran-mib threshold-overloaded	Specifies the amount of traffic that indicates the backhaul is overloaded.
	ipran-mib backhaul-notify-interval	Specifies the interval used to suppress the generation of utilization notifications.

keepalive

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

keepalive [*period* [*retries*]]

no keepalive [*period* [*retries*]]

Syntax Description

<i>period</i>	(Optional) Integer value in seconds greater than 0. The default is 10.
<i>retries</i>	(Optional) Number of times that the device will continue to send keepalive packets without response before bringing the interface down. The integer value is greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value was specified previously, the default value of 5 is used. If this command is used with a tunnel interface, then this variable specifies the number of times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down.

Defaults

period: 10 seconds

retries: 5

If you enter only the **keepalive** command with no arguments, the defaults for both arguments are used.

If you enter only the **keepalive** command and the timeout (*period*) parameter, the default number of retries (5) is used.

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	The <i>retries</i> argument was added and made available on tunnel interfaces.
12.2(8)MC2	This command was incorporated.
12.2(13)	The default value for the <i>retries</i> argument was increased to 5.
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.

Dropped Packets

Because keepalive packets are treated as ordinary packets, it is possible that they will be dropped. To reduce the possibility that dropped keepalive packets will cause the tunnel interface to be taken down, increase the number of retries.

**Note**

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

Examples

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

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

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

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

load-interval

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

load-interval *seconds*

no load-interval *seconds*

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

Defaults	<i>300 seconds (or 5 minutes)</i>
-----------------	-----------------------------------

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.

match ip dscp

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

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

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

Syntax Description

<i>ip-dscp-value</i>	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 Gigabit Ethernet 0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet 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 GigabitEthernet0/0
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.

mode y-cable

To access the command mode that allows you to manually control the relays on the voice/WAN interface card (VWIC) or high-speed WAN interface card (HWIC), use the **mode y-cable** command in redundancy configuration mode.

mode y-cable

Syntax Description This command has no parameters, it invokes the y-cable mode.

Defaults There are no default settings or behaviors.

Command Modes Redundancy configuration

Command History	Release	Modification
	12.2(8)MC2	This command was introduced.
	12.2(15)MC1	This command was incorporated.
	12.3(11)T	This command was incorporated.
	12.4(2)MR	This command was incorporated.

Examples The following example enables y-cable mode:

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

Related Commands	Command	Description
	standalone	Indicates whether the Cisco 3825 router is being used as a standalone device and manually sets the relays.
	standby use-interface	Designates a loopback interface as a health or revertive interface.
	redundancy	Invokes redundancy mode.

mpls ip

To enable MPLS forwarding of IPv4 packets along normally routed paths for a specified interface, use the **mpls ip** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

mpls ip

no mpls ip

Syntax Description

This command has no arguments or keywords.

Defaults

MPLS forwarding of IPv4 packets along normally routed paths for the interface is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4(16)MR	This command was integrated into Cisco IOS Release 12.4(16)MR.

Usage Guidelines

MPLS forwarding of IPv4 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching has been enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the **no** form of the command does not affect the sending of labeled packets through any Label Switched Path (LSP) tunnels that might use the interface.

For an LC-ATM interface, the **no** form of this command prevents the establishment of label virtual circuits (LVCs) beginning at, terminating at, or passing through the interface.

Examples

The following example shows that label switching is enabled on the specified Ethernet interface:

```
Router# config t
Router(config)# configure terminal
Router(config-if)# interface Ethernet 0/1/0
Router(config-if)# mpls ip
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
mpls ldp maxhops	Limits the number of hops permitted in an Label Switched Path (LSP) established by the downstream-on-demand method of label distribution.
show mpls interfaces	Displays information about one or more interface that has been configured for label switching.

pseudowire-class

To specify the name of a Layer 2 pseudowire-class and enter **pseudowire-class** configuration mode, use the **pseudowire-class** command in the global configuration mode.

pseudowire-class [*pw-class-name*]

Syntax Description	<i>pw-class-name</i> (Required) The name of a Layer 2 pseudowire-class.
--------------------	---

Defaults	No pseudowire-class is defined.
----------	---------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.0(23)S	This command was introduced.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines	The pseudowire-class command configures a pseudowire-class template that consists of configuration settings used by all attachment circuits bound to the class. A pseudowire-class includes the following configuration settings:
------------------	--

- Data encapsulation type
- Control protocol
- Sequencing
- IP address of the local Layer 2 interface
- Type of service (ToS) value in IP headers

After entering the **pseudowire-class** command, the router switches to pseudowire-class configuration mode where PW settings can be configured.

Examples	The following example shows how to enter pseudowire-class configuration mode to configure a PW configuration template named “ether-pw”:
----------	---

```
Router# config t
Router(config)# pseudowire-class 12tp
Router(config-pw-class)# encapsulation 12tpv3
Router(config-pw-class)# exit
Router(config)# exit
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire-classes, and then enters the L2TP-class configuration mode.
pseudowire	Binds an attachment circuit to a Layer 2 PW for an xconnect service.
xconnect	Binds an attachment circuit to an L2TPv3 PW for an xconnect service and then enters xconnect configuration mode.

pw-pvc

To configure permanent virtual circuit (PVC) mapping or rewrite the PW configured for a PVC, use the **pw-pvc** command. This command specifies the PW-side vpi/vci value to be used inside PW packet payload in sending and receiving PW packets for a specified PVC.

pw-pvc [pw-vpi]/[pw-vci]

Syntax Description

pw-vpi	Pseudowire-side vpi value
pw-vci	Pseudowire-side vci value

Defaults

By default, PW-side vpi/vci value is the same as the attachment circuit-side vpi/vci value.

Command Modes

l2transport VC mode

Command History

Release	Modification
12.4(2)MR2	This command was introduced.

Examples

The following example illustrates the use of the **pw-pvc** command.

```
Router# config t
Router(config-if)# pvc 0/40 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aa10
Router(config-if-atm-l2trans-pvc)# pw-pvc 1/40
Router(config-if-atm-l2trans-pvc)# xconnect 1.1.1.1 40 encapsulation mpls
Router(config-if-atm-l2trans-pvc-xconn)# exit
Router(config-if-atm-l2trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
xconnect	The xconnect command is used to bind an attachment circuit to a PW in one of the supported configuration modes.

redundancy

To access the command mode that allows you to configure aspects of redundancy, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description

This command has no parameters; it invokes the redundancy mode.

Defaults

There are no default settings or behaviors.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)MC2	This command was introduced.
12.2(15)MC1	This command was incorporated.
12.3(11)T	This command was incorporated.
12.4(2)MR	This command was incorporated.

Examples

The following example enables redundancy mode:

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

Related Commands

Command	Description
mode y-cable	Invokes y-cable mode.
standalone	Indicates whether the Cisco 3825 router is being used as a standalone device and manually sets the relays.
standby use-interface	Designates a loopback interface as a health or revertive interfaces.

sample-rate

To specify in milliseconds the rate hardware samples the data on the attached circuit, use the **sample-rate** command in the circuit emulation (CEM) circuit configuration mode.

sample-rate [*sample-rate*]

Syntax Description	<i>sample rate</i>	Sample rate translates into the <i>payload-size</i> sent over the circuit. The default is 1 ms.
		<ul style="list-style-type: none"> 32-timeslots at 1ms = 256-bytes (32-timeslots * 8-bytes/timeslot/ms) 24-timeslots at 2ms = 384-bytes (24-timeslots * 16-bytes/timeslot/ms)

Command Modes	CEM circuit configuration
---------------	---------------------------

Command History	Release	Modification
	12.4(12)MR2	This command was introduced.

Examples The following example illustrates the use of the **sample-rate** command:

```
Router# config t
Router(config)# interface cem 0/0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# sample-rate 2
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	cem	Apply CEM class.
	cem class	Applies the CEM interface parameters defined in the given <cem-class-name> to the circuit.
	class cem	Configure's CEM interface parameters in a class that's applied to CEM interfaces together in the global configuration mode.

scrambling-payload

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 **scrambling-payload** command in interface configuration mode. The **no** form disables scrambling.

scrambling-payload

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.4(4)MR	This command was incorporated.

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 ATM0/0/0
Router(config-if)# no ip address
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# ima-group 0
Router(config-if)# scrambling-payload
```

sequencing

To configure the direction in which sequencing is enabled for data packets in a Layer 2 PW, use the **sequencing** command in the pseudowire-class configuration mode. To remove the sequencing configuration from the pseudowire-class, use the **no** form of this command.

sequencing {**transmit** | **receive** | **both** | **resync** {*number*}}

no sequencing {**transmit** | **receive** | **both** | **resync** {*number*}}

Syntax Description	transmit	Updates the Sequence Number field in the headers of data packets sent over the PW according to the data encapsulation method that is used.
	receive	Keeps the value in the Sequence Number field in the headers of data packets received over the PW. Out-of-order packets are dropped.
	both	Enables both the transmit and receive options.
	resync	Enables the reset of packet sequencing after the disposition router receives a specified number of out-of-order packets.
	<i>number</i>	The number of out-of-order packets that cause a reset of packet sequencing. The range is 5 to 65,535.

Defaults Sequencing is disabled.

Command Modes Pseudowire-class configuration

Command History	Release	Modification
	12.0(23)S	This command was introduced for Layer 2 Tunnel Protocol Version 3 (L2TPv3).
	12.0(29)S	This command was updated to support Any Transport over MPLS (AToM).
	12.0(30)S	The resync keyword was added.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines When you enable sequencing using any of the available options, the sending of sequence numbers is automatically enabled and the remote provider edge (PE) peer is requested to send sequence numbers. Out-of-order packets received on the PW are dropped only if you use the **sequencing receive** or **sequencing both** command.

It is useful to specify the **resync** keyword for situations when the disposition router receives many out-of-order packets. It allows the router to recover from situations where too many out-of-order packets are dropped.

Set the sequence number to 0 in the slow path before packets are punted to the local CPU, because packets may become out of order.

**Note**

Sequencing will not override the value for CEM circuits.

Examples

The following example shows how to enable sequencing in data packets in Layer 2 PWs that were created from the pseudowire-class named “ether-pw” so that the Sequence Number field is updated in tunneled packet headers for data packets that are both sent and received over the PW:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# sequencing both
Router(config-pw-class)# exit
Router(config)# exit
```

The following example shows how to enable the disposition router to reset packet sequencing after it receives 1,000 out-of-order packets:

```
Router# config t
Router(config)# pseudowire-class mpls
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# sequencing both
Router(config-pw-class)# sequencing resync 1000
Router(config-pw-class)# exit
Router(config)# exit
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding (CEF) on the Route Processor card.
pseudowire-class	Specifies the name of an L2TP pseudowire-class and enters pseudowire-class configuration mode.

show atm cell-packing

To display cell packing information for the Layer 2 attachment circuits (ACs) configured on your system, use the **show atm cell-packing** command in the EXEC mode.

show atm cell-packing

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	Release 3.4.1	This command was introduced on the Cisco XR 12000 Series Router.
	12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Examples The following sample output is from the **show atm cell-packing** command:

```
Router# show atm cell-packing
```

Circuit Type		local MNC	avg # cells/pkt rcvd	negotiated MNC	avg # cells/pkt sent	MCPT (us)
ATM0/2/0/1.200	vc 1/200	1	0	1	0	50
ATM0/2/0/1.300	vc 1/300	1	0	1	0	50

Related Commands	Command	Description
	cell-packing	Packs multiple ATM cells into each MPLS or L2TPv3 packet.
	atm cell-packing	Packs multiple ATM cells into each MPLS or L2TPv3 packet.

show cem circuit

To display a summary of circuit emulation (CEM) circuits, use the **show cem circuit** command in the privileged EXEC mode.

show cem circuit [*cem-id*]

Syntax Description

<i>cem-id</i>	(Optional) Identifies the circuit configured via the cem-group configuration mode.
---------------	--

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(12)MR2	This command was introduced.

Examples

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

```
Router# show cem circuit
CEM Int.      ID   Ctrlr   Admin   Circuit   AC
-----
CEM0/0/0      0   UP      UP      Enabled   UP
CEM0/0/1      1   UP      UP      Enabled   UP
CEM0/1/0      2   UP      UP      Enabled   UP
CEM0/1/1      3   UP      UP      Enabled   UP
CEM0/2/0      4   UP      UP      Enabled   UP
CEM0/2/1      5   UP      UP      Enabled   UP
```

```
Router# show cem circuit 5
```

```
CEM0/2/1, ID: 5, Line: UP, Admin: UP, Ckt: Enabled
Controller state: up
Idle Pattern: 0xFF, Idle cas: 0x8
Dejitter: 4, Sample Rate: 1, Payload Size: 192
Framing: Framed, (DS0 channels: 1-24)
CEM Defects Set
None
```

```
Signalling: No CAS
RTP: No RTP
```

```
Ingress Pkts:    527521938      Dropped:          0
Egress Pkts:     527521938      Dropped:          0
```

```
CEM Counter Details
Input Errors:    0      Output Errors:    0
Pkts Missing:   0      Pkts Reordered:   0
Misorder Drops: 0      JitterBuf Underrun: 0
Error Sec:      0      Severly Errored Sec: 0
Unavailable Sec: 0      Failure Counts:   0
Pkts Malformed: 0
```

Related Commands	Command	Description
	show cem circuit detail	Displays detailed information about all CEM circuits.
	show cem platform	Displays platform-specific error counters for all CEM circuits.
	show cem platform errors	Displays platform-specific error counters for all CEM circuits.

show cem platform

To display platform-specific error counters for all circuit emulation (CEM) circuits, use the **show cem platform** command in the privileged EXEC mode.

show cem platform [*interface*]

Syntax Description	<i>interface</i> (Optional) Identifies the CEM interface (for example, CEM0/0/1).				
Command Modes	Privileged EXEC				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.4(12)MR2</td><td>This command was introduced.</td></tr> </table>	Release	Modification	12.4(12)MR2	This command was introduced.
Release	Modification				
12.4(12)MR2	This command was introduced.				

Examples

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

```
Router# show cem platform
CEM0/0/0 errors:
  net2cem_drops ===== 50/527658758
  net2cem_drops_underflow === 26
  net2cem_drops_overflow ==== 24
  Last cleared 6d02h
CEM0/0/1 errors:
  net2cem_drops ===== 50/527658759
  net2cem_drops_underflow === 25
  net2cem_drops_overflow ==== 25
  Last cleared 6d02h
CEM0/1/0 errors:
  net2cem_drops ===== 2/526990836
  net2cem_drops_overflow ==== 2
  Last cleared never
CEM0/1/1 errors:
  net2cem_drops ===== 1/526982274
  net2cem_drops_overflow ==== 1
  Last cleared never
CEM0/2/0 errors:
  net2cem_drops ===== 51/527658758
  net2cem_drops_underflow === 26
  net2cem_drops_overflow ==== 25
  Last cleared 6d02h
CEM0/2/1 errors:
  net2cem_drops ===== 48/527660498
  net2cem_drops_underflow === 24
  net2cem_drops_overflow ==== 24
  Last cleared 6d02h

Router# show cem platform cem0/0/1
CEM0/0/1 errors:
  net2cem_drops ===== 50/527678398
  net2cem_drops_underflow === 25
  net2cem_drops_overflow ==== 25
  Last cleared 6d02h
```

Related Commands	Command	Description
	show cem circuit	Displays a summary of CEM circuits.
	show cem circuit detail	Displays detailed information about all CEM circuits.
	show cem platform errors	Displays platform-specific error counters for all CEM circuits.

show connection

To display the status of interworking connections, use the **show connection** command in the privileged EXEC mode.

show connection [**all** | *element* | **id** *ID* | **name** *name* | **port** *port*]

Syntax Description

all	(Optional) Displays information about all interworking connections.
<i>element</i>	(Optional) Displays information about the specified connection element.
id <i>ID</i>	(Optional) Displays information about the specified connection identifier.
name <i>name</i>	(Optional) Displays information about the specified connection name.
port <i>port</i>	(Optional) Displays information about all connections on an interface. (In Cisco IOS Release 12.0S, only ATM, serial.)

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)T	This command was introduced as show connect (FR-ATM).
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S and updated to show all ATM, serial, and Fast Ethernet interworking connections.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.4(2)T	This command output was changed to add Segment 1 and Segment 2 fields for Segment state and channel ID.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(8)	This command was integrated into Cisco IOS Release 12.4(8).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows the local interworking connections on a router:

```
Router# show connection
ID   Name                Segment 1                Segment 2                State
=====
1    conn1               ATM 1/0/0 AAL5 0/100    ATM 2/0/0 AAL5 0/100    UP
2    conn2               ATM 2/0/0 AAL5 0/300    Serial0/1 16             UP
3    conn3               ATM 2/0/0 AAL5 0/400    FA 0/0.1 10             UP
4    conn4               ATM 1/0/0 CELL 0/500    ATM 2/0/0 CELL 0/500    UP
5    conn5               ATM 1/0/0 CELL 100      ATM 2/0/0 CELL 100      UP
```

Table 1 describes the significant fields shown in the display.

Table 1 *show connection Field Descriptions*

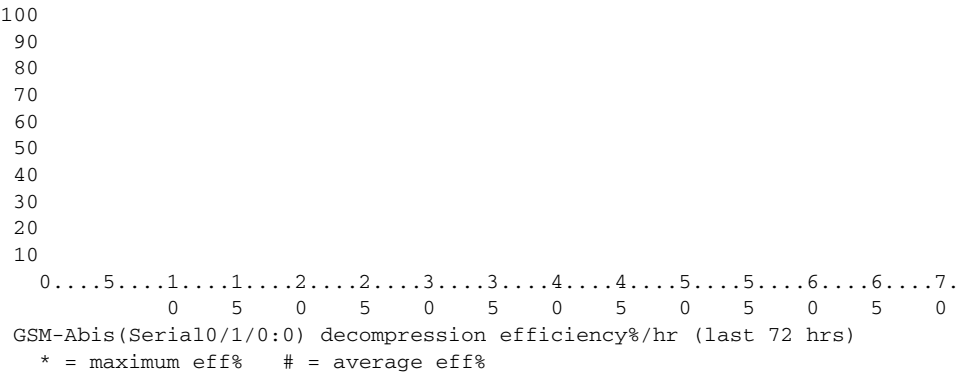
Field	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.
Segment 1 Segment 2	Information about the interworking segments, including: <ul style="list-style-type: none"> Interface name and number. Segment state, interface name and number, and channel ID. Segment state will display nothing if the segment state is UP, “-” if the segment state is DOWN, and “***Card Removed***” if the segment state is DETACHED. Type of encapsulation (if any) assigned to the interface. Permanent virtual circuit (PVC) assigned to the ATM interface, data-link connection identifier (DLCI) assigned to the serial interface, or VLAN ID assigned to the Ethernet interface.
State or Status	Status of the connection, which is one of the following: INVALID, UP, ADMIN UP, ADMIN DOWN, OPER DOWN, COMING UP, NOT VERIFIED, ERR.

Related Commands

Command	Description
connect (L2VPN local switching)	Connects two different or like interfaces on a router.
show atm pvc	Displays the status of ATM PVCs and SVCs.
show frame-relay pvc	Displays the status of Frame Relay interfaces.

Cisco 3825 Mobile Wireless Edge Router Software Configuration Guide

show gsm-abis efficiency



Related Commands	Command	Description
	clear gsm-abis	Clears the statistics displayed.

show gsm-abis errors

To display error statistics counters of 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(Serial0/1/0:0): backhaul_rxLostPakInd ===== 1/431956
GSM-Abis(Serial0/1/0:0): backhaul_txLostPakInd ===== 1/432539
GSM-Abis(Serial0/1/0:0): backhaul_missedPaks ===== 654/431956
GSM-Abis(Serial0/1/0:0): backhaul_latePaks ===== 591
GSM-Abis(Serial0/1/0:0): backhaul_lostPaks ===== 1
GSM-Abis(Serial0/1/0:0): backhaul_txRset ===== 33
GSM-Abis(Serial0/1/0:0): backhaul_overrun ===== 29
GSM-Abis(Serial0/1/0:0): compression_failures ===== 39661
GSM-Abis(Serial0/1/0:0): backhaul_congestion_drops ===== 39661
GSM-Abis(Serial0/1/0:0): backhaul_congestion_events ===== 1
GSM-Abis(Serial0/1/0:0): backhaul_congestion_duration(sec) == 80
GSM-Abis(Serial0/1/0:0): backhaul_congestion_bytes ===== 16498976
Last cleared 00:14:24
```

Table A-3 describes the significant fields shown in the display.

Table A-2 *show gsm-abis errors Field Descriptions*

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

Table A-2 *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_txPctl_no_memory	No particles available, for example, getparticle () failure.
backhaul_txReset	Packets lost due to txBufferRing reset.
decompression_failures	Decompression of input backhaulPak failed.
compression_failures	Compression of input GSM packet failed.
no-backhaul_pak_available	No memory for backhaulPak buffer.
no-backhaul_interface	Could not find an output interface that corresponds to configured remote 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 the is 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(Serial0/1/0:0): 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	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>12.4(2)MR</td><td>This command was introduced.</td></tr> </table>	Release	Modification	12.4(2)MR	This command was introduced.
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 peering ser0/1/0:0
GSM-Abis(Serial0/1/0:0): Peering Information
GSM-Abis(Serial0/1/0:0): Local (10.10.10.1:5555) States:
GSM-Abis(Serial0/1/0:0): Connect State Is: CONNECTED
GSM-Abis(Serial0/1/0:0): Local Alarm Is: CLEAR (NO ALARM)
GSM-Abis(Serial0/1/0:0): Redundancy State: ACTIVE
GSM-Abis(Serial0/1/0:0): Local Peer Version: 1.0
GSM-Abis(Serial0/1/0:0): Remote (10.10.10.2:5555) States:
GSM-Abis(Serial0/1/0:0): Remote Alarm Is: CLEAR (NO ALARM)
GSM-Abis(Serial0/1/0:0): Remote Peer Version: 1.0

Router# show gsm-abis peering detail ser0/1/0:0
GSM-Abis(Serial0/1/0:0): 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:
Retransmission Contexts Used = 1 (in use)
Data Buffers Used ===== 0 (in use)
Seq Num: tx_fsn/tx_bsn ===== 4/4
Seq Num: rx_fsn/rx_bsn ===== 4/4
Adjacent serial number: 'FTX1021A44Q'

```

Related Commands	Command	Description
	clear gsm-abis	Clears the statistics displayed.

show gsm-abis 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-abis traffic** command in privileged EXEC mode.

show gsm-abis traffic

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	Privileged EXEC
----------------------	-----------------

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

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

```
Router# show gsm-abis traffic
```

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

Related Commands	Command	Description
	clear gsm-abis	Clears the statistics displayed.

show ip rtp header-compression

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

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

Syntax Description	<i>type number</i>	(Optional) Interface type and number.
	detail	(Optional) Displays details of each connection.
	Note This keyword is not supported on the Cisco 3825 router.	

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 Multilink1 (compression off, IETF, RTP)
  Rcvd: 0 total, 0 compressed, 0 errors
        0 dropped, 0 buffer copies, 0 buffer failures
  Sent: 430 total 429 compressed
        15122 bytes saved, 0 bytes sent
        0 efficiency improvement factor
Connect: 16 rx slots, 16 tx slots, 0 long searches, 1 misses
        99% hit ratio, five minute miss rate 0 misses/sec, 0 max.
```

Table A-3 describes the significant fields shown in the display.

Table A-3 *show ip rtp header-compression Field Descriptions*

Field	Description
Interface	Type and number of 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 3825 router.
buffer failures	Not applicable to the Cisco 3825 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 3825 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 3825 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 3825 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 l2tp session

To display basic information about all active L2TP sessions, use the **show l2tp session** command in the user EXEC mode.

show l2tp session

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History	Release	Modification
	12.1(1)T	This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) information.
	12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.
	12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines Use the **show l2tp session** command to display information about all active sessions using L2TP.

Examples The following is sample output from the **show l2tp session** command on a device with active L2TP sessions:

```
Router# show l2tp session
```

```
L2TP Session Information Total tunnels 1 sessions 4
```

LocID	RemID	TunID	Username, Intf/ Vcid, Circuit	State	Last Chg	Uniq ID
9547	61932	2220	100, AT0/0:	est	2w6d	1
9580	61966	2220	1100, AT0/1:0/100	est	2w6d	21
9584	61970	2220	1200, AT0/1.1:	est	2w6d	29
9595	61981	2220	1101, AT0/1:0/101	est	1w0d	37

```
Router#
```

Related Commands	Command	Description
	show l2tp domain	Displays all VPDN domains and DNIS groups configured on the NAS.
	show l2tp group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information and current session information.
	show l2tp history failure	Displays the content of the failure history table.
	show l2tp multilink	Displays the multilink sessions authorized for all VPDN groups.

Command	Description
show l2tp redirect	Displays statistics for L2TP redirects and forwards.
show l2tp session	Displays session information about active Layer 2 sessions for a VPDN.
show l2tp tunnel	Displays information about active Layer 2 tunnels for a VPDN.

show l2tp tunnel

To display basic information about all L2TP tunnels, use the **show l2tp tunnel** command in the user EXEC mode.

show l2tp tunnel

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History	Release	Modification
	11.2	This command was integrated into Cisco IOS Release 12.4(12)MR2.
	12.1(1)T	This command was enhanced to display Point-to-Point Protocol over Ethernet (PPPoE) information.
	12.1(2)T	This command was enhanced to display PPPoE session information on actual Ethernet interfaces.
	12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines Use the **show l2tp tunnel** command to display information about all active tunnels using L2TP.

Examples The following is sample output from the **show l2tp tunnel** command on a device with active L2F and L2TP tunnels:

```
Router# show l2tp tunnel
```

```
L2TP Tunnel Information Total tunnels 1 sessions 4
```

LocID	RemID	Remote Name	State	Remote Address	Port	Sessions	L2TP Class/ VPDN Group
2220	55756	mwr2	est	99.99.99.99	0	4	l2tp_default_cl

```
Router#
Router#
Router#
Router#
```

Related Commands	Command	Description
	show l2tp domain	Displays all VPDN domains and DNIS groups configured on the network access server (NAS).
	show l2tp group	Displays a summary of the relationships among VPDN groups and customer/VPDN profiles, or summarizes the configuration of a VPDN group including DNIS/domain, load sharing information and current session information.
	show l2tp history failure	Displays the content of the failure history table.

Command	Description
show l2tp multilink	Displays the multilink sessions authorized for all VPDN groups.
show l2tp redirect	Displays statistics for L2TP redirects and forwards.
show l2tp session	Displays session information about active Layer 2 sessions for a VPDN.

show mpls l2transport vc

To display information about Any Transport over MPLS (AToM) virtual connections (VCs) that have been enabled to route Layer 2 packets on a router, use the **show mpls l2transport vc** command in the privileged EXEC mode.

```
show mpls l2transport vc {[vcid vc-id] | [vcid vc-id-min vc-id-max]} [interface name
[local-circuit-id]] [destination ip-address | name] [detail]
```

Syntax Description

vcid	(Optional) Allows you to enter a specific VC ID to display.
<i>vc-id</i>	(Optional) The VC ID number.
<i>vc-id-min</i> <i>vc-id-max</i>	(Optional) Allows you to enter a range of VCs to display. The range is from 1 to 4294967295. (This argument is primarily used for legacy implementations.)
interface	(Optional) The interface or subinterface of the router that has been enabled to transport Layer 2 packets. This keyword lets you display information about the VCs that have been assigned VC IDs on that interface or subinterface.
<i>name</i>	(Optional) The name of the interface or subinterface.
<i>local-circuit-id</i>	(Optional) The number assigned to the local circuit. This argument value is supported only by the following transport types: <ul style="list-style-type: none"> For ATM adaptation layer 5 (AAL5) and cell relay, enter the virtual path identifier (VPI)/virtual channel identifier (VCI) of the PVC. For Ethernet VLANs, enter the VLAN number.
destination	(Optional) Information about the VCs that have been assigned VC IDs for the remote router you specify.
<i>ip-address</i>	(Optional) The IP address of the remote router.
<i>name</i>	(Optional) The name assigned to the remote router.
detail	(Optional) Detailed information about the VCs that have been assigned VC IDs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)E	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was implemented on the Cisco 10720 router.
12.0(23)S	The interface and destination keywords were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was implemented on Cisco 7304 routers.
12.0(25)S	This command was updated with new output and fields to display information about tunnel selection and ATM cell relay port mode.

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2 SX.
12.2(25)S	This command was updated with new output and fields for nonstop forwarding (NSF), stateful switchover (SSO), and graceful restart (GR) abilities.
12.2(28)SB	This command was implemented on the Cisco 10000 series routers. Example output was changed for the Cisco 10000 series router, and two fields (SSO Descriptor and SSM segment/switch IDs) were removed from the output because they are not supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(16)MR	This command was integrated into Cisco IOS Release 12.4(16)MR.

Usage Guidelines

If you do not specify any keywords or arguments, the command displays a summary of all the VCs.

Examples

The output of the commands varies, depending on the type of Layer 2 packets being transported over the AToM VCs.

The following sample output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router:

Router# **show mpls l2transport vc**

Local intf	Local circuit	Dest address	VC ID	Status
AT4/0	ATM AAL5 0/100	10.0.0.1	100	UP
AT4/0	ATM AAL5 0/200	10.0.0.1	200	UP
AT4/0.300	ATM AAL5 0/300	10.0.0.1	300	UP

Table A-4 describes the significant fields shown in the display.

Table A-4 *show mpls l2transport vc Field Descriptions*

Field	Description
Local intf	The interface on the local router that has been enabled to transport Layer 2 packets.
Local circuit	The type and number (if applicable) of the local circuit. The output shown in this column varies, depending on the transport type: <ul style="list-style-type: none"> For ATM cell relay and AAL5, the output shows the VPI/VCI of the PVC. For Ethernet VLANs, the output shows the VLAN number.
Dest address	The IP address of the remote router's interface that is the other end of the VC.
VC ID	The VC identifier assigned to one of the interfaces on the router.

Table A-4 *show mpls l2transport vc Field Descriptions (continued)*

Field	Description
Status	<p>The status of the VC. The status can be one of the following:</p> <ul style="list-style-type: none"> • UP—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed. <ul style="list-style-type: none"> – The disposition interface is programmed if the VC has been configured and the client interface is up. – The imposition interface is programmed if the disposition interface is programmed and you have a remote VC label and an Interior Gateway Protocol (IGP) label. The IGP label can be implicit null in a back-to-back configuration. An IGP label means there is a Label Switched Path (LSP) to the peer. • DOWN—The VC is not ready to carry traffic between the two VC endpoints. Use the detail keyword to determine the reason that the VC is down. • ADMIN DOWN—The VC has been disabled by a user. • RECOVERING—The VC is recovering from a stateful switchover.

The following example shows information about the NSF/SSO and graceful restart capability. The SSO portion indicates when checkpointing data has either been sent (on active) or received (on standby). When SSO data has not been successfully sent or has been released, the SSO information is not shown.

Router# **show mpls l2transport vc detail**

```

Local interface: Fa0/1.1 down, line protocol down, Eth VLAN 2 up
  Destination address: 10.55.55.2, VC ID: 1002, VC status: down
    Output interface: Fa0/0, imposed label stack {16}
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop point2point
  Create time: 02:03:29, last status change time: 02:03:26
  Signaling protocol: LDP, peer 10.55.55.2:0 down
    MPLS VC labels: local 16, remote unassigned
    Group ID: local 0, remote unknown
    MTU: local 1500, remote unknown
    Remote interface description:
  Sequencing: receive disabled, send disabled
  SSO Descriptor: 10.55.55.2/1002, local label: 16
    SSM segment/switch IDs: 12290/8193, PWID: 8193
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0

```

Table A-5 describes the significant fields shown in the display.

Table A-5 *show mpls l2transport vc Field Descriptions*

Field	Description
line protocol	Status of the line protocol on the edge-facing interface.
Destination address	IP address of the remote router specified for this VC. Specify the destination IP address as part of the mpls l2transport route command.

Table A-5 *show mpls l2transport vc Field Descriptions (continued)*

Field	Description
Local interface	Interface on the local router that has been enabled to send and receive Layer 2 packets. The interface varies, depending on the transport type. The output also shows the status of the interface.
VC ID	VC identifier assigned to the interface on the router.
VC status	<p>Status of the VC, which is one of the following:</p> <p>UP—The VC is in a state where it can carry traffic between the two VC endpoints. A VC is up when both imposition and disposition interfaces are programmed.</p> <ul style="list-style-type: none"> The disposition interface is programmed if the VC has been configured and the client interface is up. The imposition interface is programmed if the disposition interface is programmed and a remote VC label and an IGP label exist. The IGP label can be an implicit null in a back-to-back configuration. (An IGP label means there is an LSP to the peer.) <p>DOWN—The VC is not ready to carry traffic between the two VC endpoints.</p> <p>ADMIN DOWN—The VC has been disabled by a user.</p>
Output interface	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
imposed label stack	Summary of the MPLS label stack used to direct the VC to the PE router.
Preferred path	Path that was assigned to the VC and the status of that path. The path can be an MPLS traffic engineering tunnel or an IP address or hostname of a PE router.
Default path	<p>Status of the default path, which can be disabled or active.</p> <p>By default, if the preferred path fails, the router uses the default path. However, you can disable the router from using the default path when the preferred path fails by specifying the disable-fallback keyword with the preferred-path command.</p>
Create time	Time when the VC was provisioned.
last status change time	Last time the VC state changed.
Signaling protocol	Type of protocol used to send the MPLS labels. The output also shows the status of the peer router.
MPLS VC labels	Local VC label is a disposition label, which determines the egress interface of an arriving packet from the MPLS backbone. The remote VC label is a disposition VC label of the remote peer router.
Group ID	Local group ID is used to group VCs locally. The remote group ID is used by the peer to group several VCs.
MTU	Maximum transmission unit specified for the local and remote interfaces.
Remote interface description	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
Sequencing	Indicates whether sequencing of out-of-order packets is enabled or disabled.

Table A-5 *show mpls l2transport vc Field Descriptions (continued)*

Field	Description
Tunnel label	<p>An IGP label used to route the packet over the MPLS backbone to the destination router with the egress interface. The first part of the output displays the type of label. The second part of output displays the route information.</p> <p>The tunnel label information can display any of the following states:</p> <ul style="list-style-type: none"> • imp-null—The provider (P) router is absent and the tunnel label is not to be used. Alternatively, imp-null can signify traffic engineering tunnels between the PE routers. • unassigned—The label has not been assigned. • no route—The label is not in the routing table. • no adjacency—The adjacency for the next hop is missing. • not ready, no route—An IP route for the peer does not exist in the routing table. • not ready, not a host table—The route in the routing table for the remote peer router is not a host route. • not ready, Cisco Express Forwarding disabled—Cisco Express Forwarding is disabled. • not ready, LFIB disabled—The MPLS switching subsystem is disabled. • not ready, label forwarding information base (LFIB) entry present—The tunnel label exists in the LFIB, but the VC is down.
SSO Descriptor	Identifies the VC for which the information was checkpointed.
local label	The value of the local label that was checkpointed (that is, sent on the active Route Processor [RP], and received on the standby RP).
SSM segment/switch IDs	The IDs used to refer to the control plane and data plane contexts for this VC. This data is not for customer use but for Cisco personnel for troubleshooting purposes. When the source specific multicast (SSM) IDs are followed by the word "used," the checkpointed data has been successfully sent and not released.
PWID	The PW ID used in the data plane to correlate the switching context for the segment mentioned with the MPLS switching context. This data is not for customer use but for Cisco personnel for troubleshooting purposes.
packet totals	Number of packets sent and received. Received packets are those AToM packets received from the MPLS core. Sent packets are those AToM packets sent to the MPLS core. This does not include dropped packets.
byte totals	Number of bytes sent and received from the core-facing interface, including the payload, control word if present, and AToM VC label.
packet drops	Number of dropped packets.

Related Commands

Command	Description
show mpls l2transport summary	Displays summary information about VCs that have been enabled to route AToM Layer 2 packets on a router.

show redundancy

To display information about the current redundant configuration and recent changes in states, use the **show redundancy** command in privileged EXEC mode.

show redundancy

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(8)MC2	This command was introduced.
	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 In the **standby group name group-name** command, if you omit the *group-name* or if you enter a group name that does not begin with 1 or 2, the configuration will fail and there will be a mismatch in the information displayed by the **show redundancy** and **show standby** commands.

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

```
Router# show redundancy
MWR3825 is the Active Router
Previous States with most recent at bottom

INITL_INITL      Dec 31 19:00:00.000
LISTN_INITL      Feb 28 19:00:15.568
LISTN_LISTN      Feb 28 19:00:15.568
SPEAK_LISTN      Feb 28 19:00:18.568
SPEAK_SPEAK      Feb 28 19:00:18.568
STDBY_SPEAK      Mar 19 08:54:26.191
ACTIV_SPEAK      Mar 19 08:54:26.191
ACTIV_STDBY      Mar 19 08:54:26.191
ACTIV_ACTIV      Mar 19 08:54:26.191
INITL_ACTIV      Mar 19 08:56:22.700
INITL_INITL      Mar 19 08:56:22.700
INITL_LISTN      Mar 19 08:56:28.544
LISTN_LISTN      Mar 19 08:56:28.652
LISTN_SPEAK      Mar 19 08:56:31.544
SPEAK_SPEAK      Mar 19 08:56:31.652
SPEAK_STDBY      Mar 19 08:56:34.544
SPEAK_ACTIV      Mar 19 08:56:34.544
STDBY_ACTIV      Mar 19 08:56:34.652
ACTIV_ACTIV      Mar 19 08:56:34.652
INITL_ACTIV      Mar 19 10:20:41.455
INITL_INITL      Mar 19 10:20:41.455
INITL_LISTN      Mar 19 10:20:49.243
```

```

LISTN_LISTN      Mar 19 10:20:49.299
LISTN_SPEAK      Mar 19 10:20:52.244
SPEAK_SPEAK      Mar 19 10:20:52.300
SPEAK_STDBY      Mar 19 10:20:55.244
STDBY_STDBY      Mar 19 10:20:55.300
ACTIV_STDBY      Mar 19 10:21:01.692
ACTIV_ACTIV      Mar 19 10:21:01.692

```

Related Commands

Command	Description
mode y-cable	Invokes y-cable mode.
redundancy	Invokes redundancy mode.
standalone	Specifies whether the Cisco 3825 router is used in a redundant or standalone configuration.
standby	Sets HSRP attributes.
standby use-interface	Specifies the interfaces to be used for health and revertive interfaces.

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 0/0/1
UMTS(ATM0/0/1):
  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	<p>The following is an example of the output generated by this command.</p> <pre>Router# show umts eff Router# show umts efficiency atm 0/0/1 UMTS(ATM0/0/1): efficiency (1sec/5sec/1min/5min/1hr) units(%%) decompression efficiency (100/100/100/100/---) compression efficiency (100/100/100/100/---)</pre>	
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 0/0/1
UMTS-Iub(ATM0/0/1): 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 0/0/1
UMTS-Iub(ATM0/0/1):      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(ATM1/1/1): backhaul_peer_not_ready ===== 6
UMTS-Iub(ATM1/1/1): no_remote_pvc ===== 6
UMTS-Iub(ATM1/1/1): backhaul_invalid_pak ===== 1
UMTS-Iub(ATM1/1/1): decompression_failures ===== 1
UMTS-Iub(ATM1/1/1):      no_shorthaul_pak_available == 1
UMTS-Iub(ATM1/1/1): compression_failures ===== 1
UMTS-Iub(ATM1/1/1):      no_backhaul_pak_available == 1
UMTS-Iub(ATM1/1/1):      no_backhaul_interface ===== 1
UMTS-Iub(ATM1/1/1):      backhaul_interface_down ===== 1
```



```

UMTS-Iub(ATM1/1/1):    backhaul_encap_failures ===== 1
UMTS-Iub(ATM1/1/1):    umts_encap_failures ===== 1
UMTS-Iub(ATM1/1/1):    no_local_pvc ===== 1
UMTS-Iub(ATM1/1/1):    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 0/1/0
UMTS-Iub(ATM0/1/0): 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 Multi-Link Point-to-Point Protocol (MLPPP) backhauls and for other backhaul interfaces, such as GE, 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.
	12.4(4)MR	This command added IMA in the output, how traffic for a PVC is off loaded to an alternate backhaul, and how alarms are carried over primary backhaul.

Examples

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

Example 1

```
Router# show umts peering atm 0/0/1
UMTS-Iub(ATM0/0/1): Peering Information
UMTS-Iub(ATM0/0/1):      Local (40.40.40.40:6666) States:
UMTS-Iub(ATM0/0/1):      Connect State: OPEN
UMTS-Iub(ATM0/0/1):      Redundancy State: ACTIVE
UMTS-Iub(ATM0/0/1):      Alarm State: RX(NO ALARM)          TX(NO ALARM)
UMTS-Iub(ATM0/0/1):Version: 1
UMTS-Iub(ATM0/0/1):      Remote (40.40.40.41:6666) States:
UMTS-Iub(ATM0/0/1):      Alarm State: RX(NO ALARM)          TX(NO ALARM)
UMTS-Iub(ATM0/0/1):      Version: 1
```

Example 2

```
Router# show umts peering detail atm 0/0/1
UMTS-Iub(ATM0/0/1): Peering Information (Version 1)
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 with IMA

```

Router# show umts peering
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0): Peering Information
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Local (20.20.20.21:6666) States:
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Connect State: OPEN
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Redundancy State: ACTIVE
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Version: 4
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Alarm State:
UMTS-Iub(ATM0/0/0 - ATM0/0/0): RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/0/1 - ATM0/0/1): RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Remote (20.20.20.20:6666) States:
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Version: 4
UMTS-Iub(ATM0/IMA0 - ATM0/IMA0):      Alarm State:
UMTS-Iub(ATM0/0/0 - ATM0/0/0):      RX(NO ALARM)      TX(NO ALARM)
UMTS-Iub(ATM0/0/1 - ATM0/0/1):      RX(NO ALARM)      TX(NO ALARM)

```



Note

In the previous output, the local shorthaul/interface name appears before the dash (–), and the remote shorthaul/interface name appears after the dash (–).

Example 4 with Alternate Backhaul (192.168.10.2 to 192.168.10.1)

```

Router# show umts peering
UMTS-Iub(ATM0/IMA0): Peering Information
UMTS-Iub(ATM0/IMA0):      Local (20.20.20.21:6666) States:
UMTS-Iub(ATM0/IMA0):      Connect State: OPEN
UMTS-Iub(ATM0/IMA0):      Redundancy State: ACTIVE
UMTS-Iub(ATM0/IMA0):      Version: 3
UMTS-Iub(ATM0/IMA0):      Alarm State:
UMTS-Iub(ATM0/0/0) ID(1):      RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/0/1) ID(2):      RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/IMA0):      Remote (20.20.20.20:6666) States:
UMTS-Iub(ATM0/IMA0):      Version: 3

```

```

UMTS-Iub(ATM0/IMA0):      Alarm State:
UMTS-Iub(ATM0/0/0) ID(1):      RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/0/1) ID(2):      RX(NO ALARM) TX(NO ALARM)

UMTS-Iub(ATM0/IMA0.1): Peering Information
UMTS-Iub(ATM0/IMA0.1):      Local (192.168.10.2:6666) States:
UMTS-Iub(ATM0/IMA0.1):      Connect State: OPEN
UMTS-Iub(ATM0/IMA0.1):      Redundancy State: ACTIVE
UMTS-Iub(ATM0/IMA0.1):      Version: 3
UMTS-Iub(ATM0/IMA0.1):      Remote (192.168.10.1:6666) States:
UMTS-Iub(ATM0/IMA0.1):      Version: 3

```

Example 5 with Alarms over Primary Backhaul

```

Router# show umts peering
UMTS-Iub(ATM0/IMA0): Peering Information
UMTS-Iub(ATM0/IMA0):      Local (20.20.20.21:6666) States:
UMTS-Iub(ATM0/IMA0):      Connect State: OPEN
UMTS-Iub(ATM0/IMA0):      Redundancy State: ACTIVE
UMTS-Iub(ATM0/IMA0):      Version: 3
UMTS-Iub(ATM0/IMA0):      Alarm State:
UMTS-Iub(ATM0/0/0) ID(1):      RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/0/1) ID(2):      RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/IMA0):      Remote (20.20.20.20:6666) States:
UMTS-Iub(ATM0/IMA0):      Version: 3
UMTS-Iub(ATM0/IMA0):      Alarm State:
UMTS-Iub(ATM0/0/0) ID(1):      RX(NO ALARM) TX(NO ALARM)
UMTS-Iub(ATM0/0/1) ID(2):      RX(NO ALARM) TX(NO ALARM)

UMTS-Iub(ATM0/IMA0.1): Peering Information
UMTS-Iub(ATM0/IMA0.1):      Local (192.168.10.2:6666) States:
UMTS-Iub(ATM0/IMA0.1):      Connect State: OPEN
UMTS-Iub(ATM0/IMA0.1):      Redundancy State: ACTIVE
UMTS-Iub(ATM0/IMA0.1):      Version: 3
UMTS-Iub(ATM0/IMA0.1):      Remote (192.168.10.1:6666) States:
UMTS-Iub(ATM0/IMA0.1):      Version: 3

```

Example 6 with Congestion Control Status

```

Router# show umts-iub peering atm 0/ima0
UMTS-Iub(ATM0/IMA0): Peering Information
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Local (20.20.20.21:6666) States:
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Connect State: OPEN
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Redundancy State: ACTIVE
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Congestion Control: ON
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Version: 4
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Alarm State:
UMTS-Iub(ATM0/0/0 - ATM0/2):      RX(NO ALARM)      TX(NO ALARM)
UMTS-Iub(ATM0/0/1 - ATM0/3):      RX(NO ALARM)      TX(NO ALARM)
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Remote (20.20.20.20:6666) States:
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Version: 4
UMTS-Iub(ATM0/IMA0 - ATM0/IMA1):      Alarm State:
UMTS-Iub(ATM0/0/0 - ATM0/2):      RX(NO ALARM)      TX(NO ALARM)
UMTS-Iub(ATM0/0/1 - ATM0/3):      RX(NO ALARM)      TX(NO ALARM)

```

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.

show umts-iub pvc

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(ATM0/0/1): 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)
```

show umts-iub 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-iub traffic** command in privileged EXEC mode.

show umts-iub 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-iub traffic

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

Related Commands	Command	Description
	clear umts-iub	Clears the statistics displayed.

show xconnect all

To display information about xconnect attachment circuits and pseudowires (PWs), use the **show xconnect all** command in the privileged EXEC mode.

show xconnect [**all** | **interface** *interface* | **peer** *ip-address* {**all** | **vcid** *vcid*}] [**detail**]

Syntax Description

all	Displays information about all xconnect attachment circuits and PWs.
interface <i>interface</i>	Displays information about xconnect attachment circuits and PWs on the specified interface. Valid values for the interface argument are as follows: <ul style="list-style-type: none"> atm number—Displays xconnect information for a specific ATM interface or subinterface. atm number vp vpi-value—Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). This command does not display information about virtual connection (VC) xconnects using the specified VPI. atm number vp vpi-value/vci-value—Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination. ethernet number—Displays port-mode xconnect information for a specific Ethernet interface or subinterface. fastethernet number—Displays port-mode xconnect information for a specific Fast Ethernet interface or subinterface. serial number—Displays xconnect information for a specific serial interface. serial number dlci-number—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).
peer ip-address { all vcid <i>vcid</i> }	Displays information about xconnect attachment circuits and PWs associated with the specified peer IP address. <ul style="list-style-type: none"> all—Displays all xconnect information associated with the specified peer IP address. vcid vcid—Displays xconnect information associated with the specified peer IP address and the specified VC ID.
detail	(Optional) Displays detailed information about the specified xconnect attachment circuits and PWs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.4(16)MR	This command was integrated into Cisco IOS Release 12.4(16)MR.

Usage Guidelines

The **show xconnect all** command can be used to display, sort, and filter basic information about all xconnect attachment circuits and PWs.

You can use the **show xconnect all** command output to help determine the appropriate steps to troubleshoot an xconnect configuration problem. More specific information about a particular type of xconnect can be displayed using the commands listed in the Related Commands table.

Examples

The following example shows **show xconnect all** command output in the brief (default) display format.

The sample output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router:

```
Router# show xconnect all
```

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State

UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware

XC ST	Segment 1	S1 Segment 2	S2
UP ac	Et0/0(Ethernet)	UP mpls 10.55.55.2:1000	UP
UP ac	Et1/0.1:200(Eth VLAN)	UP mpls 10.55.55.2:5200	UP
IA pri ac	Et1/0.2:100(Eth VLAN)	UP ac Et2/0.2:100(Eth VLAN)	UP
UP sec ac	Et1/0.2:100(Eth VLAN)	UP mpls 10.55.55.3:1101	UP

Table A-6 describes the significant fields shown in the display.

Table A-6 *show xconnect all Field Descriptions*

Field	Description
XC ST	<ul style="list-style-type: none"> State of the xconnect attachment circuit or PW. Valid states are: UP—The xconnect attachment circuit or PW is up. Both segment 1 and segment 2 must be up for the xconnect to be up. DN—The xconnect attachment circuit or PW is down. Either segment 1, segment 2, or both segments are down. IA—The xconnect attachment circuit or PW is inactive. This state is valid only when PW redundancy is configured. NH—One or both segments of this xconnect no longer has the required hardware resources available to the system.
Segment1 or Segment2	<p>Information about the type of xconnect, the interface type, and the IP address the segment is using. Types of xconnects are:</p> <ul style="list-style-type: none"> ac—Attachment circuit. pri ac—Primary attachment circuit. sec ac—Secondary attachment circuit. mpls—Multiprotocol Label Switching. l2tp—Layer 2 Tunnel Protocol.

Table A-6 *show xconnect all Field Descriptions (continued)*

Field	Description
S1	State of the segment. Valid states are:
or	
S2	
	<ul style="list-style-type: none"> UP—The segment is up. DN—The segment is down. AD—The segment is administratively down.

The following example shows **show xconnect all** command output in the detailed display format:

Router# **show xconnect all detail**

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State

UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No HardwareXC

ST	Segment 1	S1 Segment 2	S2
UP	ac Et0/0 (Ethernet) Interworking: ip	UP mpls 10.55.55.2:1000 Local VC label 16 Remote VC label 16 pw-class: mpls-ip	UP
UP	ac Et1/0.1:200 (Eth VLAN) Interworking: ip	UP mpls 10.55.55.2:5200 Local VC label 17 Remote VC label 20 pw-class: mpls-ip	UP
IA pri	ac Et1/0.2:100 (Eth VLAN) Interworking: none	UP ac Et2/0.2:100 (Eth VLAN) Interworking: none	UP
UP sec	ac Et1/0.2:100 (Eth VLAN) Interworking: none	UP mpls 10.55.55.3:1101 Local VC label 23 Remote VC label 17 pw-class: mpls	UP

The additional fields displayed in the detailed output are self-explanatory.

Related Commands

Command	Description
show atm pvc	Displays all ATM PVCs and traffic information.
show atm vc	Displays all ATM PVCs and SVCs and traffic information.
show atm vp	Displays the statistics for all VPs on an interface or for a specific VP.
show connect	Displays configuration information about drop-and-insert connections that have been configured on a router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show l2tun session	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
show mpls l2transport binding	Displays VC label binding information.
show mpls l2transport vc	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

snmp-server enable traps ipran

To enable all ipran notifications 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

Related Commands This command has no arguments or keywords.

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

Command Modes Global configuration

Command History	Release	Modification
	12.4(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

This statement controls the generation of the cisco IpRanBackHaulGsmAlarm notification from the CISCO-IP-RAN-BACKHAUL-MIB.

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.4(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-umts notifications, use the **no** form of this command.

snmp-server enable traps ipran alarm-umts

no snmp-server enable traps ipran alarm-umts

This statement controls the generation of the cisco IpRanBackHaulUmtsAlarm notification from the CISCO-IP-RAN-BACKHAUL-MIB.

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.4(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.
12.4(9)MR	Support for utilization notification has been removed and the command is provided only to maintain compatibility.

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.
ipran-mib backhaul-notify-interval	Specifies the interval used to calculate the utilization.
ipran-mib threshold-acceptable	Specifies the acceptable level of traffic.
ipran-mib threshold-overloaded	Specifies the amount of traffic that indicates the backhaul is overloaded.
ipran-mib threshold-warning	Specifies the amount of traffic that indicates the backhaul is carrying traffic sufficient to impact performance, but is not overloaded.

standalone

To specify that the Cisco 3825 router is being used in a standalone configuration (which impacts the relays on the VWIC/HWIC), use the **standalone** command in y-cable configuration mode. To use the router in a redundant configuration, use the **no** form of this command.

[no] standalone

Syntax Description This command has no arguments or keywords.

Defaults By default, the Cisco 3825 router is configured to be used in a redundant configuration (**no standalone**) and the relays are open.

Command Modes Y-cable configuration

Command History	Release	Modification
	12.2(8)MC2	This command was introduced.
	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 Issuing the **standalone** command closes the relays on the VWICs/HWICs installed in the Cisco 3825 router.

Examples The following example closes the relays so that the router can be used as a standalone device.

```
Router# standalone
```

Related Commands	Command	Description
	mode y-cable	Invokes y-cable mode.
	standby use-interface	Specifies the interfaces to be used for health and revertive interfaces.

standby use-interface

To designate a loopback interface as a health or revertive interface, use the **standby use-interface** command in y-cable configuration mode.

standby use-interface *interface* {**health** | **revertive** | **backhaul**}

Syntax Description

<i>interface</i>	Interface to be used with the specified parameter. For health and revertive , this is the loopback interface that is specified in the standby track command. For backhaul , the interface must be an MLPPP interface. If you want to use a serial interface as the backhaul, you must first configure that interface to be part of an MLPPP bundle.
health	Interface that will the router for an overtemperature condition, the state of the processor, and the state of the T1/E1 firmware. If any of these conditions indicates a failure, this interface is brought down. Otherwise, the health interface remains in the up state.
revertive	Interface that acts as the revertive interface. If the Cisco 3825 router changes state from active to standby, the revertive interface is brought up. If the router changes state from standby to active, the revertive interface is brought down.
backhaul	Interface to be used for backhauling.

Defaults

By default, the Cisco 3825 is configured to be used in a redundant configuration (**no standalone**) and the relays are open.

Command Modes

Y-cable configuration

Command History

Release	Modification
12.2(8)MC2	This command was introduced.

Usage Guidelines

The loopback interfaces that you specify for the health and revertive interfaces must be the same loopback interfaces that you specified in the **standby track** command. In the **standby track** command, the decrement value for the revertive interface should always be less than that for other interfaces. We recommend that you use loopback101 for health and loopback102 for revertive.

The interface that you specify for the backhaul must be an MLPPP interface. If you want to use a serial interface as the backhaul, you must first configure that interface to be part of an MLPPP bundle. We recommend you that use multilink1 for the backhaul interface.

Examples

The following example specifies loopback101 as the health interface and loopback102 as the revertive interface:

```
Router# standby use-interface loopback101 health
Router# standby use-interface loopback102 revertive
Router# standby use-interface multilink1 backhaul
```

Related Commands

Command	Description
mode y-cable	Invokes y-cable mode.
redundancy	Invokes redundancy mode.
standalone	Specifies whether the Cisco 3825 router is used in a redundant or stand-alone configuration.
standby	Sets HSRP attributes.

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 3825 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 3825 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 ATM0/2/0
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-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 3825 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 (GE), 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 was introduced.

Examples

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

```
Router(config)# interface a0/3/0
Router(config-if) umts-iub backhaul-timer ?
<1-8> timer value(in msec)
Router(config-if)#
```

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 was 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 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	<i>protected</i>	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 was 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 local

To configure the local parameters required to establish an Internet Protocol/User Datagram 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.
<i>port</i>	(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 ATM0/2/0
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 Datagram 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	(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 ATM0/2/0
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

<i>value</i>	A number from 0 to 63 or hex value that sets the UMTS-Iub DSCP value.
--------------	---

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the parameters:

```
Router(config)# interface ATM0/2/0
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 <i>value</i> 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

<i>value</i>	A number from 0 to 63 or hex value that sets the UMTS-Iub DSCP value.
--------------	---

Defaults

There are no default settings or behaviors.

Command Modes

ATM-VC configuration

Command History

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

Examples

The following example shows how to configure the remote parameters:

```
Router(config)# interface ATM0/2/0
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 <i>value</i> 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

<i>value</i>	A number from 0 to 63 that sets the UMTS-Iub DSCP value.
--------------	--

Defaults

There are no default settings or behaviors.

Command Modes

Interface configuration

Command History

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

Examples

The following example shows how to configure the parameters:

```
Router(config)# interface ATM0/2/0
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 <i>value</i> for UMTS shorthaul interfaces and is used to tag the backhaul packet generated from traffic from a PVC

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 was introduced.

Examples

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

```
Router(config)# interface ATM0/2/0
Router(config-if)# atm umts-iub
Router(config-subif)# atm umts
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
atm umts	This command enables the UMTS mode for alternate backhaul.
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 was introduced.

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

```
Router(config)# interface ATM0/2/0
Router(config-if)# atm umts-iub
Router(config-subif)# atm umts
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
	atm umts	This command enables the UMTS mode for alternate backhaul.
	umts local [ip-address]	This command configures the remote IP address for alternate backhaul.

xconnect

To bind an attachment circuit to a pseudowire (PW), use the **xconnect** command in one of the supported configuration modes. To restore the default values, use the **no** form of this command.

xconnect *peer-ip-address* | *vcid* | *pseudowire-parameters* [**sequencing** { **transmit** | **receive** | **both** | **one-to-one** }] [**ignore-vpi-vci**]

Syntax Description	
<i>peer-ip-address</i>	IP address of the remote provider edge (PE) peer.
<i>vcid</i>	The 32-bit identifier of the virtual circuit between the PE routers.
<i>pseudowire-parameters</i>	Encapsulation and pseudowire-class parameters to be used for the attachment circuit. At least one of the following PW parameters must be configured: <ul style="list-style-type: none"> • encapsulation { l2tpv3 mpls }— Specifies the tunneling method to encapsulate the data in the PW: <ul style="list-style-type: none"> – l2tpv3—Specifies L2TPv3 as the tunneling method. – mpls—Specifies MPLS as the tunneling method. • pw-class <i>pw-class-name</i>—Specifies the pseudowire-class configuration from which the data encapsulation type is taken. This option is mandatory if you select an encapsulation method.
sequencing	(Optional) Sets the sequencing method to be used for packets received or sent.
	 Note Sequencing is not supported for CEM circuits.
transmit	Sequences data packets received from the attachment circuit.
receive	Sequences data packets sent into the attachment circuit.
both	Sequences data packets that are both sent and received from the attachment circuit.
one-to-one	Only apply when the xconnect command is configured under the AAL0 encapsulation PVC. It specifies the PW type as a one-to-one VCC cell relay.
ignore-vpi-vci	With the ignore-vpi-vci keyword configured, the MWR ignores the VPI/VCi value in the PW packet and does a blind rewrite with the local configured AC-side PVC's VPI/VCi value. Only apply when the xconnect command is configured under the PVC, which is the N:1 with N=1 special case. Do not apply when the xconnect command is configured under the subinterface, which supports N>1.

Defaults The attachment circuit is not bound to the PW.

Command Modes

- CEM circuit configuration
- Interface configuration
- Subinterface configuration

l2transport configuration (for ATM)

Connect configuration mode Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.0(28)S	Support was added for Multilink Frame Relay connections.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(12)MR2	This command was integrated into Cisco IOS Release 12.4(12)MR2.

Usage Guidelines

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each xconnect configuration must have a unique combination of peer-ip-address and vcid configuration.



Note

If the remote router is a Cisco 12000 series Internet router, the *peer-ip-address* argument must specify a loopback address on the router.

The same vcid value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE router. The vcid creates the binding between a PW and an attachment circuit.

The **pw-class** pw-class-name value binds the xconnect configuration of an attachment circuit to a specific pseudowire-class. In this way, the pseudowire-class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **xconnect** command.



Note

If you specify the encapsulation keywords, you must specify the **pw-class** keyword.

Keyword ignore-vpi-vci

Using the **xconnect** command with keyword **ignore-vpi-vci** provides benefits over using the **pw-pvc** command for PVC mapping.

Originally, PVC mapping was done through the **pw-pvc pw-vpi/pw-vci** command. When the MWR received the MPLS PW packet, it decoded the PW payload and looked up the PW VPI/VCI value to see if it matched any local configured PVC values. If a match was made, the PW-VPI/PW-VCI was translated to the AC-side VPI/VCI and the cell was sent to the local PVC. Without a match, the MWR dropped the received PW packet. When the MWR generated the PW packet, it used configured **pw-vpi/pw-vci** values. In this case, the PVC mapping was done completely on the MWR and was transparent to the remote end.

The scenario differs when keyword **ignore-vpi-vci** is configured. For N:1 with N=1 special case, when the PW packet is received from the MWR, the receiving router ignores the VPI/VCI value contained in the PW payload. It does a blind rewrite to use the AC-side VPI/VCI and sends the cell to the AC side PVC.

The **xconnect** command with keyword **ignore-vpi-vci** results in the PVC mapping being done in a cooperative way if the MWR works the same way as the receiving router. Without this command, the MWR checks the VPI/VCI value inside PW packet for matches against the local configured PVC or PVC-mapping. With the **ignore-vpi-vci** keyword configured, the MWR ignores the VPI/VCI header inside the received PW packet and does a blind rewrite with the local configured AC-side PVC's VPI/VCI value.

**Note**

This applies only to N:1 VCC PW with N=1 special case.

Examples

The following example illustrates the configured **xconnect** service for an ATM interface by binding the ATM circuit to the PW named 123 with a remote peer 10.0.3.201. The configuration settings in the pseudowire-class named ATM-xconnect are used.

```
Router# config t
Router(config)# interface ATM 0/0/0
Router(config-if)# xconnect 10.0.3.201 123 pw-class ATM-xconnect
Router(config-if-xconn)# exit
Router(config-if)# exit
Router(config)# exit
```

The following example illustrates PVC mapping using the keyword **ignore-vpi-vci** with the **xconnect** command. The example shows both the MWR and remote end (7600) routers.

MWR:

```
Router# config t
Router(config)# interface ATM 0/0
Router(config-if)# pvc 0/10 12transport
Router(config-if-atm-12trans-pvc)# encapsulation aa10
Router(config-if-atm-12trans-pvc)# xconnect 10.10.10.10 100 encapsulation mpls ignore-vpi-vci
Router(config-if-atm-12trans-pvc-xconn)# exit
Router(config-if-atm-12trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

7600:

```
Router# config t
Router(config)# interface ATM 0/0
Router(config-if)# pvc 2/20 12transport
Router(config-if-atm-12trans-pvc)# encapsulation aa10
Router(config-if-atm-12trans-pvc)# xconnect 20.20.20.20 100 encapsulation mpls
Router(config-if-atm-12trans-pvc-xconn)# exit
Router(config-if-atm-12trans-pvc)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
show xconnect	Displays information about xconnect attachment circuits and PWs.
pseudowire-class	Configures a template of PW configuration settings used by the attachment circuits transported over a PW.

xconnect logging redundancy

To enable system message log (syslog) reporting of the status of the xconnect redundancy group, use the **xconnect logging redundancy** command in global configuration mode. To disable syslog reporting of the status of the xconnect redundancy group, use the **no** form of this command.

xconnect logging redundancy

no xconnect logging redundancy

Syntax Description

This command has no arguments or keywords.

Defaults

Syslog reporting of the status of the xconnect redundancy group is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(16)MR	This command was integrated into Cisco IOS Release 12.4(16)MR.

Usage Guidelines

Use this command to enable syslog reporting of the status of the xconnect redundancy group.

Examples

The following example enables syslog reporting of the status of the xconnect redundancy group and shows the messages that are generated during switchover events:

```
Router# config t
Router(config)# xconnect logging redundancy
Router(config)# exit
```

Activating the Primary Member

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

Activating the Backup Member:

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

Related Commands

Command	Description
xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an L2TPv3 PW for xconnect service and enters xconnect configuration mode.