APPENDIX A

Cisco MWR 2941-DC Router RAN-O Command Reference

This appendix contains an alphabetical listing of new and revised commands specific to the Cisco MWR 2941-DC router in a RAN-O solution.

- ipran-mib location
- ipran-mib snmp-access
- ipran-mib threshold-acceptable
- ipran-mib threshold-overloaded
- ipran-mib threshold-warning
- keepalive
- load-interval
- match ip dscp
- mpls ip
- network-clock-select hold_timeout
- network-clock-select input-stratum4
- network-clock-select mode
- network-clock-select priority
- payload-size
- pseudowire-class
- ptp announce
- ptp clock-source
- ptp clock-destination
- ptp delay-req
- ptp domain
- ptp enable
- ptp master
- ptp mode
- ptp priority1
- ptp priority2
- ptp slave
- ptp sync interval
- ptp sync limit
- pw-pvc
- recovered-clock slave
- recovered-clock recovered
- set network-clocks
- show atm cell-packing
- show cem circuit
- show cem platform
- show connection
- show controller
- show gsm-abis efficiency

- show gsm-abis errors
- show gsm-abis packets
- show gsm-abis peering
- show gsm-abis traffic
- show interface switchport backup
- show ip rtp header-compression
- show mpls l2transport vc
- show network-clocks
- show platform hardware
- show ptp clock
- show ptp foreign-master-record
- show ptp parent
- show ptp port
- show ptp time-property
- show xconnect all
- snmp-server enable traps ipran
- snmp-server enable traps ipran alarm-gsm
- snmp-server enable traps ipran util
- switchport backup interface
- xconnect
- xconnect logging redundancy

backup delay

To specify how long a backup pseudowire (PW) virtual circuit (VC) should wait before resuming operation after the primary PW VC goes down, use the **backup delay** command in interface configuration mode or xconnect configuration mode. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

backup delay *enable-delay* {*disable-delay* | **never**}

no backup delay *enable-delay* {*disable-delay* | **never**}

Syntax Description

enable-delay	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.
disable-delay	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
12.4(19)MR2	This command was incorporated.

Examples

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

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

The following example shows an MPLS xconnect with one redundant peer. The switchover does not begin unless the PW has been down for 3 seconds. After a switchover to the secondary VC occurs, there is no fallback to the primary until the primary VC has been reestablished and is up for 10 seconds.

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

Related Commands

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

backup peer

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

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

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

Syntax Description

peer-router-ip-addr	IP address of the remote peer.
vcid	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.
pw-class-name	(Optional) Name of the PW you created when you established the PW class.

Defaults

No redundant peer is established.

Command Modes

Interface configuration

Xconnect configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

Examples

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

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

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

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

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

Related Commands

Command	Description
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

no cdp enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled at the global level and on all supported interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
cdp run	Reenables 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

group-number	CEM identifier to be used for this group of time slots: • 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 *time-slot-range* argument. *time-slot-range*—Specifies the time slots to be included in the CEM channel. The list of time slots may include commas and hyphens with no spaces between the numbers.

Defaults

No CEM groups are defined.

Command Modes

Controller configuration

Command History

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

Usage Guidelines

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

Examples

The following example shows how to create a CEM channel:

SATOP

```
Router# config t
Router(config)# controller e1 0/0
Router(config-controller)# cem-group 0 unframed
Router(config-controller)# exit
Router(config)# interface cem 0/0
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
```

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

CESoPSN

```
Router# config t
Router(config)# controller e1 0/1
Router(config-controller)# cem-group 0 timeslots 1-31
Router(config-controller)# exit
Router(config)# interface cem 0/1
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.

class cem

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

class cem *class-name*

Syntax Description

class-name	The name of a CEM interface parameters class.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **class cem** command allows you to configure CEM interface parameters in a class that is applied to CEM interfaces together. A **class cem** command includes the following configuration settings:

- **dejitter-buffer** *dejitter-in-ms*
- **idle-pattern** *8-bit-idle-pattern*
- **payload-size** *payload-size-in-ms*

Note You can improve the performance of packet reordering on TDM/PWE connections by using the increasing the size of the dejitter buffer using the **dejitter-buffer** parameter.

Examples

The following example shows how to configure CEM interface parameters:

```
Router# config t
Router(config)# class cem mycemclass
Router(config-cem-class)# dejitter-buffer 10
Router(config-cem-class)# sample-rate 32
Router(config-cem-class)# exit
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# cem class mycemclass
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
dejitter-buffer	Specifies the size of the dejitter buffer used for network jitter in CEM configuration mode.
idle-pattern	Specifies the data pattern to transmit on the T1/E1 line when missing packets are detected on the PWE3 circuit in CEM configuration mode.
sample-rate	Specifies in milliseconds the rate hardware samples the data on the attached circuit in 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	
serial-number	(Optional) The serial number range is from 0 to 6.
interface-number	(Optional) The interface number range is from 0 to 6.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to clear statistics:

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

Related Commands

Command	Description
show gsm-abis efficiency	Displays the history of GSM compression/decompression efficiency averages at intervals of 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour.
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
12.4(19)MR2	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.

dejitter-buffer

To configure the size of the dejitter buffer, use the **dejitter-buffer** command in CEM configuration mode. To restore the dejitter buffer to its default size, use the **no** form of this command.

dejitter-buffer *size*

no dejitter-buffer

Syntax Description

size	Specifies the size of the dejitter buffer in milliseconds. The range is 4 to 500 ms; the default is 4 ms.

Defaults

The default dejitter-buffer size is 4 milliseconds.

Command Modes

CEM configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to specify the size of the dejitter buffer:

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# dejitter-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	Configures CEM interface parameters in a class that's applied to CEM interfaces together in global configuration mode.

gsm-abis congestion abate

To set the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated, use the **gsm-abis congestion abate** interface configuration command. The abatement detection level is defined as *x* milliseconds of continuous congestion abatement (that is, no congestion indications).

gsm-abis congestion abate *ms*

Syntax Description

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to set the abatement detection level to 250 ms:

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

Related Commands

Command	Description
gsm-abis congestion critical	Defines the critical time slots 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 router when congestion is detected.
gsm-abis congestion onset	Sets the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.
gsm-abis local	Configures the local parameters for an IP/UDP backhaul connection.
gsm-abis remote	Configures the remote parameters for an IP/UDP backhaul connection.

gsm-abis congestion critical

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

gsm-abis congestion critical *time-slot-range*

Syntax Description

time-slot-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.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to set the time-slot range:

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

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router stops suppressing time slots 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 router when congestion is detected.
gsm-abis congestion onset	Sets the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.
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

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

gsm-abis congestion enable

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to enable the congestion detection algorithm:

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

Related Commands

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

To set the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion, use the **gsm-abis congestion onset** interface configuration command. The onset detection level is defined as *x* milliseconds of continuous congestion detected.

gsm-abis congestion onset *ms*

Syntax Description

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

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

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

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated.
gsm-abis congestion critical	Defines the critical time slots 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 router when congestion is detected.
gsm-abis jitter	Sets the amount of transmit jitter delay for the GSM-Abis interface.
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

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

gsm-abis jitter *ms*

Syntax Description

ms	Sets the number of milliseconds for the jitter. The default value is 4 ms. Valid values are 4–500 ms.

Defaults

The default jitter value is 4 ms.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

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

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

Related Commands

Command	Description
gsm-abis congestion abate	Sets the congestion abatement detection level at which the remote router stops suppressing time slots because congestion has been alleviated.
gsm-abis congestion critical	Defines the critical time slots 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 router when congestion is detected.
gsm-abis congestion onset	Sets the congestion onset detection level at which the remote router starts suppressing all time slots that are not defined as critical in an effort to alleviate congestion.

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

gsm-abis local

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

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

Syntax Description

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to configure the local parameters:

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

Related Commands

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

gsm-abis lost-recovery

This command allows you to control the speed at which the router retransmits subrate data for lost packets. This method of retransmission prevents large retransmission packets from delaying subsequent backhaul packets.

To set the retransmission rate for subrate data for the lost packets, use the **gsm-abis lost-recovery** configuration command.

gsm-abis lost-recovery *milliseconds*

Syntax Description

milliseconds	The retransmission rate for subrate data, in milliseconds. Range is 0-5000.
	Note Any value under 40 causes the router to send all subrates at once when lost packet is indicated, effectively disabling the feature.

Defaults

The default setting is gsm-abis lost-recovery 1250.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to configure the remote parameters:

```
Router(config)# interface Serial10/2.0
Router(config-if)# encapsulation gsm-abis
Router(config-if)# gsm-abis remote 10.10.10.1 5504
Router(config)# gsm-abis lost-recovery 1250
```

Related Commands

Command	Description
gsm-abis retransmit	Enables retransmission of a repetitive subrate sample.

gsm-abis remote

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

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

Syntax Description

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to configure the remote parameters:

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

Related Commands

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

gsm-abis retransmit

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

gsm-abis retransmit *sample-delay*

Syntax Description

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

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

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

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 subrate samples retransmitted.

gsm-abis set dscp

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

gsm-abis set dscp *value*

Note Use this command when configuring GSM shorthaul interfaces.

Syntax Description

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to mark a packet:

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

idle-pattern

To specify the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit, use the **idle-pattern** command in CEM configuration mode. To stop sending idle pattern data, use the **no** form of this command.

idle-pattern [*pattern*]

no idle-pattern

Syntax Description

pattern	(Optional) An 8-bit hexadecimal number that is transmitted as the idle pattern. T1 and E1 channels require only this argument.

Defaults

For T1 or E1 channels, the default idle pattern is 0xFF.

Command Modes

CEM circuit configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

Examples

The following example shows how to specify a data pattern:

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

Related Commands

Command	Description
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	Configures CEM interface parameters in a class that's applied to CEM interfaces together in global configuration mode.

ima-group

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

ima-group *group-number*

no ima-group *group-number*

Syntax Description

group-number	Specifies an IMA group number from 0 to 3. IMA groups can span multiple ports on a port adapter or shared port adapter (SPA) but cannot span port adapters or SPAs.

Defaults

No IMA groups are defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

Use the **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
Router(config-if)# no ip address
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# ima-group 0
```

Related Commands

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

interface atm ima

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

interface atm *slot*/**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

The interface includes individual ATM links, but no IMA groups.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

When a port is configured for IMA functionality, it no longer operates as an individual ATM link. Specifying ATM links as members of a group using the **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 an ATM interface.
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 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

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

Defaults

No IP address is configured.

Command Modes

Pseudowire-class configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
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.

Command	Description
interface atm	Configures physical links for an ATM interface.
show ima interface atm	Displays general and detailed information about IMA groups and the links they include.

ip rtp header-compression

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

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

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

Syntax Description

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
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

passive Keyword

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

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

iphc-format Keyword

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

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

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

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

ietf-format Keyword

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

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

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

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

Support for Serial Lines

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

Unicast or Multicast RTP Packets

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

Examples

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

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

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

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

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

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

Related Commands

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

ip tcp header-compression

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

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

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

Syntax Description

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

Defaults

Disabled.

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

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

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

passive Keyword

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

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

iphc-format Keyword

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

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

ietf-format Keyword

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

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

Examples

The following example sets the first serial interface for header compression with a maximum of 10 cache entries:

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

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

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

The following example enables RTP header compression on the Seria1/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified.

```
Router(config)# interface serial1/0.0
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
```

Related Commands

Command	Description
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.

ipran-mib backhaul-notify-interval

To specify the interval used to suppress the generation of the ciscoIpRanBackHaulRcvdUtil and the ciscoIpRanBackHaulSentUtil notifications from the CISCO-IP-RAN-BACKHAUL-MIB, use the **ipran-mib backhaul-notify-interval** command in global configuration mode. To remove the interval, use the **no** form of the command.

ipran-mib backhaul-notify-interval *interval*

no ipran-mib backhaul-notify-interval *interval*

Notifications are suppressed for the number of seconds specified. Notifications are not suppressed when this keyword is set to zero. The minimum interval is 1 minute and the maximum is 15 minutes. When suppression is enabled, notifications are generated when a worse state is encountered. For example, the following transitions generate notifications:

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

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

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

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

Syntax Description

interval	60 to 900 seconds, or 0 (zero).

Defaults

The default interval is 0 (notifications are not suppressed).

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to set the notification-suppression interval:

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

Related Commands

Command	Description
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

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

ipran-mib location {**addSite** | **cellSite** | **undefined**}

Syntax Description

addSite	Locates the device at a BSC or RNC site.
cellSite	Locates the device at a BTS or Node B site.
undefined	Specifies an undefined location for the device.

Defaults

The default location is cellSite.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to define the device location:

```
Router# config t
Router(config)# ipran-mib location aggSite
Router(config)# ipran-mib location cellSite
Router(config)# ipran-mib location undefined
Router(config)# no ipran-mib location
Router(config)# exit
```

Related Commands

Command	Description
ipran-mib snmp-access	Defines the type of connectivity between the device and the network management system.

ipran-mib snmp-access

To define the type of connectivity between the device and the network management system, use the **ipran-mib snmp-access** command in global configuration mode. The command is used to limit the amount of traffic while the network is in the process of in-band polling.

ipran-mib snmp-access {**inBand** | **outOfBand** | **undefined**}

Syntax Description

inBand	Defines in-band SNMP connectivity.
outOfBand	Defines out-of-band SNMP connectivity.
undefined	Specifies undefined connectivity.

Defaults

The default access type is inBand.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to define the connectivity type:

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

Related Commands

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

ipran-mib threshold-acceptable

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

ipran-mib threshold-acceptable [*utilization-percentage*]

Syntax Description

utilization-percentage	(Optional) Specifies the utilization threshold as a percentage. The range is 20 to 100 percent.

Defaults

The default threshold is 60 percent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to set the utilization threshold:

```
Router# config t
Router(config)# ipran-mib threshold-acceptable 50
Router(config)# ipran-mib threshold-acceptable 70
Router(config)# no ipran-mib threshold-acceptable
Router(config)# exit
```

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

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

ipran-mib threshold-overloaded [*utilization-percentage*]

Syntax Description

utilization-percentage	(Optional) Specifies the utilization threshold as a percentage. The range is 40 to 100 percent.

Defaults

The default threshold is 80 percent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to set the utilization threshold:

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

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

To specify a level of traffic where the instances of the cirbhBackHaulRcvdUtilState and cirbhBackHaulSentUtilState objects are marked as "warning," use the **ipran-mib threshold-warning** command in global configuration mode

All changes to this threshold take effect at the end of the current interval. The value for this object must be greater than the value specified for the **ipran-mib threshold-acceptable** command. Also, the value for this object must be less than or equal to the value of the cirbhBackHaulOverloadedThreshold object. This parameter corresponds to the cirbhBackHaulWarningThreshold object.

ipran-mib threshold-warning [*utilization-percentage*]

Syntax Description

utilization-percentage	(Optional) Specifies the utilization threshold as a percentage. The range is 30 to 100 percent.

Defaults

The default threshold is 70 percent.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to set the utilization threshold:

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

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

period	(Optional) Integer value in seconds, that represents the time interval between messages sent by the Cisco IOS software to ensure that a network interface is alive. The value must be greater than 0, and the default is 10.
retries	(Optional) Number of times that the device will continue to send keepalive packets without response before bringing the interface down. The integer value is greater than 1 and less than 255. If omitted, the value that was previously set is used; if no value was specified previously, the default value of 5 is used. If this command is used with a tunnel interface, then this variable specifies the number of times that the device will continue to send keepalive packets without response before bringing the tunnel interface protocol down.

Defaults

period: 10 seconds

retries: 5

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

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

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

Keepalive Time Interval

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

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

Line Failure

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

Keepalive Packets with Tunnel Interfaces

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

Dropped Packets

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

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

Examples

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

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

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

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

load-interval

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

load-interval *seconds*

no load-interval *seconds*

Syntax Description

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

Defaults

The default is 300 seconds (5 minutes).

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

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

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

Syntax Description

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

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(19)MR2	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 an *ip-dscp-value* of 2 is different from a packet marked with an *ip-dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of QoS policies in policy-map class configuration mode.

Examples

The following example shows how to configure the service policy called priority55 and attach service policy priority55 to an interface. In this example, the class map called ipdscp15 evaluates all packets entering interface Fast Ethernet 0/0 for an IP DSCP value of 15. If the incoming packet has been marked with the IP DSCP value of 15, the packet is treated with a priority level of 55.

```
Router(config)# class-map ipdscp15
Router(config-cmap)# match ip dscp 15
Router(config-cmap)# exit
Router(config)# policy-map priority55
Router(config-pmap)# class ipdscp15
Router(config-pmap-c)# priority55
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa0/0
Router(config-if)# service-policy input priority55
```

Related Commands

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

mpls ip

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

mpls ip

no mpls ip

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

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

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

Examples

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

```
Router# config t
Router(config)# configure terminal
Router(config-if)# interface Ethernet 0/2
Router(config-if)# mpls ip
Router(config-if)# exit
Router(config)# exit
```

Related Commands

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

network-clock-select hold_timeout

The **network-clock-select hold_timeout** command specifies how long the router waits before reevaluating the network clock entry. To remove a **network-clock-select hold_timeout** configuration, use the **no** form of this command.

network-clock-select hold_timeout {*timeout* | **infinite**}

no network-clock-select hold_timeout {*timeout* | **infinite**}

Syntax Description

timeout	A value in seconds that specifies how long the router waits before reevaluating the network clock entry. Valid values are a number from 0–86400.
infinite	Specifies an infinite holdover.

Defaults

The default setting is **network-clock-select hold_timeout infinite**.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock-select hold_timeout 2000
Router(config)# exit
```

Related Commands

Command	Description
set network-clock-select force-reselect	Forces the router to re-select the network clock.

network-clock-select input-stratum4

The **network-clock-select input-stratum4** command allows you to downgrade a clock source from Stratum3 to Stratum 4. To configure a clock source as Stratum 3, use the **no** form of this command.

network-clock-select input-stratum4

no network-clock-select input-stratum4

Defaults

The default setting is for onboard E1/T1 ports is Stratum 3; the default setting for E1/T1 HWIC ports is Stratum 4.

Note You cannot configure E1/T1 HWIC ports as Stratum3.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock-select input-stratum4
Router(config)# exit
```

Related Commands

Command	Description
set network-clock-select force-reselect	Forces the router to re-select the network clock.

network-clock-select mode

The **network-clock-select mode** command specifies the router switching mode. To remove a **network-clock-select mode** configuration, use the **no** form of this command.

network-clock-select mode {revert | nonrevert}

no network-clock-select mode {revert | nonrevert}

Syntax Description

nonrevert	Sets the network clock to non-revertive mode.
revert	Sets the network clock to revertive mode.

Defaults

The default setting is **network-clock-select mode nonrevert**.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock-select mode revert
Router(config)# exit
```

Related Commands

Command	Description
set network-clock-select force-reselect	Forces the router to re-select the network clock.

network-clock-select priority

The **network-clock-select** command names a source to provide timing for the network clock and to specify the selection priority for the clock source. To remove a network-clock-select configuration, use the **no** form of this command.

network-clock-select *priority* **{bits | synce {port} | packet_timing} {E1 | T1** *slot/port***}**

no network-clock-select ***priority*** **{bits | synce {port} | packet_timing} {E1 | T1** *slot/port***}**

Syntax Description

priority	A numeric value from 1–22 that specifies the priority of the clock source.
bits	Specifies timing from a BITS port clock.
synce	Specifies timing using synchronous Ethernet.
port	Specifies the port on which synchronous Ethernet is enabled.
packet_timing	Enables packet timing using the RTM module.
E1	Specifies clocking via an E1 interface.
T1	Specifies clocking via a T1 interface.
slot/port	Specifies the slot and port of the interface used for timing.

Defaults

There is no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to use the **network-clock-select** command:

```
Router# config t
Router(config)# network-clock-select 1 packet_timing
Router(config)# exit
```

Related Commands

Command	Description
set network-clock-select force-reselect	Forces the router to re-select the network clock.

payload-size

Specifies the size of the payload for packets on a structured CEM channel.

payload-size [*payload-size*]

Syntax Description

payload-size	Specifies the size of the payload for packets on a structured CEM channel. Valid values are 32–512. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256 bytes. **Note** The payload size must be a multiple of the number of timeslots for the CEM channel. The default payload size is calculated as follows: 8 x number of timeslots x 1 ms packetization delay

Defaults

The default payload size for a structured CEM channel depends on the number of timeslots that constitute the channel. The default payload size for a T1 is 192 bytes; the default size for an E1 is 256 bytes.

Command Modes

CEM circuit configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

The Cisco MWR 2941-DC only supports a payload size of 486 (625 packets per second) or 243 (1250 packets per second).

Examples

The following example shows how to specify a sample rate:

```
Router# config t
Router(config)# interface cem 0/0
Router(config-if)# no ip address
Router(config-if)# cem 0
Router(config-if-cem)# payload-size 256
Router(config-if-cem)# xconnect 10.10.10.10 200 encapsulation mpls
Router(config-if-cem-xconn)# exit
Router(config-if-cem)# exit
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
dejitter-buffer	Configures the size of the dejitter buffer on a CEM channel.
idle-pattern	Specifies the data pattern transmitted on the T1/E1 line when missing packets are detected on the PWE3 circuit.

pseudowire-class

To specify the name of a Layer 2 pseudowire-class and enter pseudowire-class configuration mode, use the **pseudowire-class** command in global configuration mode. To remove a pseudowire class configuration, use the **no** form of this command.

pseudowire-class *pw-class-name*

no pseudowire-class *pw-class-name*

Syntax Description

pw-class-name	The name of a Layer 2 pseudowire-class.If you want to configure more than one pseudowire class, define a class name using the *pw-class-name* parameter.

Defaults

No pseudowire-class is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

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

The local interface name for each pseudowire class configured between a pair of PE routers can be the same or different.

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

Examples

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

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

Related Commands

Command	Description
pseudowire	Binds an attachment circuit to a Layer 2 PW for an xconnect service.
xconnect	Binds an attachment circuit to an Layer 2 PW for an xconnect service and then enters xconnect configuration mode.

ptp announce

Sets interval and timeout values for PTP announcement packets.

ptp announce interval *interval-value* **timeout** *timeout-value*

no ptp announce interval *interval-value* **timeout** *timeout-value*

Syntax Description

interval	Specifes the interval for PTP announce messages. The intervals are set using log base 2 values, as follows: 4—1 packet every 16 seconds 3—1 packet every 8 seconds 2—1 packet every 4 seconds 1—1 packet every 2 seconds 0—1 packet every second -1—1 packet every 1/2 second, or 2 packets per second -2—1 packet every 1/4 second, or 4 packets per second -3—1 packet every 1/8 second, or 8 packets per second -4—1 packet every 1/16 seconds, or 16 packets per second. -5—1 packet every 1/32 seconds, or 32 packets per second. -6—1 packet every 1/64 seconds, or 64 packets per second. The recommended value is -6.
timeout	Specifies the number of PTP announcement intervals before the session times out. Valid values are 2–10.

Defaults

The default interval value is 1. The default timeout value is 3.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

The recommended interval value is -6.

Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp announce interval 3
```

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

Related Commands

Command	Description
ptp enable	Enables PTP mode on an interface.

ptp clock-source

Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode.

ptp clock-source *clock-ip-address*

no ptp clock-source *clock-ip-address*

Syntax Description

clock-ip-address	The IP address of the clock source.

Defaults

The default setting is **no ptp clock-source**.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to configure a PTP clock source:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp clock-source 192.168.1.1
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp enable	Enables PTP mode on an interface.
ptp mode	Specifies the PTP mode.
ptp slave	Sets an interface to slave clock mode for PTP clocking.

ptp clock-destination

Specifies the IP address of a clock destination. This command applies only when the router is in PTP master unicast mode.

ptp clock-destination *clock-ip-address*

no ptp clock-destination *clock-ip-address*

Syntax Description

clock-ip-address	The IP address of the clock destination.

Defaults

There is no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

If the router is set to ptp master unicast, you can only configure a single destination. If the router is set to ptp master unicast negotiation, you can configure up to 128 clock destinations.

Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp clock-destination 192.168.1.2
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp enable	Enables PTP mode on an interface.
ptp master	Sets an interface in master clock mode for PTP clocking
ptp mode	Specifies the PTP mode.

ptp delay-req

Specifies the delay request interval, the time recommended to member devices to send delay request messages when an interface is in PTP master mode.

ptp delay-req interval *interval-value*

no ptp delay-req interval *interval-value*

Syntax Description

interval	Specifies the interval for delay request messages. The intervals are set using log base 2 values, as follows: 4—1 packet every 16 seconds 3—1 packet every 8 seconds 2—1 packet every 4 seconds 1—1 packet every 2 seconds 0—1 packet every second -1—1 packet every 1/2 second, or 2 packets per second -2—1 packet every 1/4 second, or 4 packets per second -3—1 packet every 1/8 second, or 8 packets per second -4—1 packet every 1/16 seconds, or 16 packets per second. -5—1 packet every 1/32 seconds, or 32 packets per second. -6—1 packet every 1/64 seconds, or 64 packets per second. The recommended value is -6.

Defaults

The default setting is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

The recommended interval value is -6.

Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp delay-req interval -4
Router(config-if)# exit
```

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

Related Commands

Command	Description
ptp enable	Enables PTP mode on an interface.
ptp master	Sets an interface in master clock mode for PTP clocking
ptp mode	Specifies the PTP mode.

ptp domain

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

ptp domain *domain-number*

no ptp domain *domain-number*

Syntax Description

domain-number	The PTP domain that the router applies to PTP traffic. Valid values are from 0–127.

Defaults

The default setting is **ptp domain 0**.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to set the ptp domain:

```
Router# config t
Router# ptp domain 88
Router(config)# exit
```

Related Commands

Command	Description
ptp enable	Enables PTP mode on an interface.
ptp mode	Specifies the PTP mode.

ptp enable

Enables PTP mode on an interface.

ptp enable

no ptp enable

Defaults

PTP is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp enable
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp master	Sets an interface in master clock mode for PTP clocking
ptp mode	Specifies the PTP mode.
ptp slave	Sets an interface to slave clock mode for PTP clocking.

ptp master

Sets an interface in master clock mode for PTP clocking. To enable ordinary master clock mode, use the **ptp master** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ptp master multicast {*unicast* | **unicast negotiation**}

no ptp master multicast {*unicast* | **unicast negotiation**}

Syntax Description

multicast	Sets the interface to use multicast mode for PTP clocking.
unicast	Sets the interface to use unicast mode for PTP clock. **Note** If the router is set to ptp master unicast, you can only configure a single destination.
unicast negotiation	Sets the interface to negotiate unicast mode for PTP clocking. **Note** If the router is set to ptp master unicast negotiation, you can configure up to 128 clock destinations.

Defaults

There is no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

For unicast and unicast negotiation, you must configure the ip address of the remote slave using the **ptp clock-destination** command before enabling PTP.

Examples

The following example shows how to enable ptp master multicast mode:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp master multicast
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp clock-destination	Specifies the IP address of a clock destination when the router is in PTP master mode.
ptp enable	Enables PTP mode on an interface.
ptp mode	Specifies the PTP mode.

ptp mode

Specifies the PTP mode.

ptp mode [ordinary]

no ptp mode [ordinary]

Note The Cisco MWR 2941-DC does not currently support other PTP modes such as boundary or transport mode.

Syntax Description

ordinary	Sets the interface to PTP clocking mode to ordinary.

Defaults

The default setting is **ptp mode ordinary**.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to enable ptp mode:

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

Related Commands

Command	Description
ptp enable	Enables PTP mode on an interface.
ptp master	Sets an interface in master clock mode for PTP clocking
ptp slave	Sets an interface to slave clock mode for PTP clocking.

ptp priority1

Sets the preference level for a clock; slave devices use the priority1 value when selecting a master clock. The priority1 value is considered above all other clock attributes. Use the following commands to set the ptp priority1 value.

ptp priority1 *priorityvalue*

no ptp priority1 *priorityvalue*

Syntax Description

priorityvalue	Valid values are from 0–255. The default value is 128.

Defaults

The default value is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to enable ptp priority1 value:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp priority1 128
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp priority2	Sets the PTP priority2 value.

ptp priority2

Sets a secondary preference level for a clock; slave devices use the priority2 value when selecting a master clock. The priority2 value is considered only when the router is unable to use priority2 and other clock attributes to select a clock. Use the following commands to set the ptp priority2 value.

ptp priority2 *priorityvalue*

no ptp priority2 *priorityvalue*

Syntax Description

priorityvalue	Valid values are from 0–255. The default value is 128.

Defaults

The default value is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to configure the ptp priority2 value:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp priority2 128
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp priority1	Sets the PTP priority1 value.

ptp slave

Sets an interface to slave clock mode for PTP clocking. To enable ordinary slave clock mode, use the **ptp slave** command in interface configuration mode. To disable this feature, use the feature, use the **no** form of this command.

ptp slave {multicast | unicast | unicast negotiation}

no ptp slave {multicast | unicast | unicast negotiation}

Syntax Description

multicast	Sets the interface to use multicast mode for PTP clocking.
unicast	Sets the interface to use unicast mode for PTP clocking.
unicast negotiation	Sets the interface to negotiate unicast mode for PTP clocking.

Defaults

There is no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

You must configure the IP address of the remote timing device before enabling PTP.

Examples

The following example shows how to enable ptp slave multicast mode:

```
Router# config t
Router# interface Vlan10
Router(config-if)# ptp slave multicast
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp clock-source	Specifies the IP address of the clock source. This command only applies when the router is in PTP slave mode.
ptp enable	Enables PTP mode on an interface.
ptp mode	Specifies the PTP mode.

ptp sync interval

Defines the interval that the router uses to send PTP synchronization messages.

ptp sync interval *interval-value*

no ptp sync interval *interval-value*

Syntax Description

interval-value	Specifies the interval at which the router sends announcement packets. The intervals are set using log base 2 values, as follows: 4—1 packet every 16 seconds 3—1 packet every 8 seconds 2—1 packet every 4 seconds 1—1 packet every 2 seconds 0—1 packet every second -1—1 packet every 1/2 second, or 2 packets per second -2—1 packet every 1/4 second, or 4 packets per second -3—1 packet every 1/8 second, or 8 packets per second -4—1 packet every 1/16 seconds, or 16 packets per second. -5—1 packet every 1/32 seconds, or 32 packets per second. -6—1 packet every 1/64 seconds, or 64 packets per second. The recommended value is -6.

Defaults

There is no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

We do not recommend that you alter the default value for the **limit** parameter.

Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp sync interval -4
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp sync limit	Defines the offset values that the router uses to send PTP synchronization messages.

ptp sync limit

Defines the offset values that the router uses to send PTP synchronization messages.

ptp sync limit *limit-value*

no ptp sync limit *limit-value*

Syntax Description

limit-value	Specifies the maximum clock offset value before PTP attempts to resynchronize. Values are in nanoseconds; the default value is 8000.

Defaults

The default value is 8000.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

We do not recommend that you alter the default value for the **limit** parameter unless suggested by Cisco support.

Examples

The following example shows how to configure a PTP announcement:

```
Router# config t
Router(config)# interface vlan 10
Router(config-if)# ptp sync limit 8000
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
ptp sync interval	Defines the interval that the router uses to send PTP synchronization messages.

pw-pvc

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

pw-pvc *pw-vpi/pw-vci*

Syntax Description

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

Defaults

The PW-side VPI/VCI value is the same as the attachment circuit-side VPI/VCI value.

Command Modes

l2transport VC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to use the **pw-pvc** command:

```
Router# config t
Router(config-if)# pvc 0/40 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aal0
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	Binds an attachment circuit to a PW in one of the supported configuration modes.

recovered-clock slave

To configure out-of-band clock recovery, use the **recovered-clock slave** command. This command automatically creates a virtual-cem interface. To access the virtual-cem interface, use the command **interface virtual-cem 0/24**. To disable this feature, use the feature, use the **no** form of this command.

recovered-clock slave

no recovered-clock slave

Defaults

There is no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to use the **recovered-clock slave** command and how to configure the virtual-cem interface:

```
Router# config t
Router(config)# recovered-clock slave
Router(config-if)# interface virtual-cem 0/24
Router(config-if)# payload-size 486
Router(config-if)# cem 0
Router(config-if)# xconnect 10.10.10.2 7600 encap mpls
Router(config-if)# exit
Router(config)# exit
```

Related Commands

Command	Description
recovered-clock recovered	Configures adaptive clock recovery.

recovered-clock recovered

The **recovered-clock recovered** command allows you to configure in-band pseudowire-based active clock recovery on a CEM interface. To disable this feature, use the feature, use the **no** form of this command.

recovered-clock recovered adaptive cem *subslot-number port-number cem-group-number*

no recovered-clock recovered adaptive cem *subslot-number port-number cem-group-number*

Syntax Description

adaptive	Specifies the clock recovery type.
cem	Specifies the Circuit emulation (CEM) interface for the recovered clock.
subslot-number	The subslot of the CEM interface for the recovered clock.
port-number	The port number of the CEM interface for the recovered clock.
cem-group-number	The CEM group to which the clock applies.

Defaults

There is no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Usage Guidelines

For more information about adaptive clock recovery, see Configuring Network Clocking Support, page 4-6.

Examples

The following example shows how to use the **recovered-clock recovered** command:

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

Related Commands

Command	Description
recovered-clock slave	Allows you to configure out-of-band clock recovery,

set network-clocks

This command causes the router to reselect a network clock; the router selects a new clock based on clock priority.

set network-clock-select [force-reselect | next-select]

Syntax Description

force-reselect	Forces the router to select a new network clock.
next-select	Forces the router to select the next available network clock.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was introduced.

Examples

The following example shows how to use the set network-clock-select force-reselect command:

```
Router# set network-clock-select force-reselect
```

Related Commands

Command	Description
show network-clocks	Displays information about all clocks configured on the router.

show atm cell-packing

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

show atm cell-packing

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows output from the **show atm cell-packing** command:

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

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

Related Commands

Command	Description
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 CEM circuits, use the **show cem circuit** command in privileged EXEC mode.

show cem circuit [*cem-id*]

Syntax Description

cem-id	(Optional) Identifies the circuit configured with the **cem-group** command.

Command Modes

Privileged EXEC

Command History Gl

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

Examples

The following examples show the output generated by this command;

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

Router# show cem circuit 5

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

Signalling: No CAS
RTP: No RTP

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

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

Related Commands

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

show cem platform

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

show cem platform [*interface*]

Syntax Description

interface	(Optional) Identifies the CEM interface (for example, CEM0/1).

Command Modes

Privileged EXEC

Command History

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

Examples

The following examples show the output generated by this command:

```
Router# show cem platform
CEM0/0 errors:
  net2cem_drops =============== 50/527658758
    net2cem_drops_underflow === 26
    net2cem_drops_overflow ==== 24
  Last cleared 6d02h
CEM0/1 errors:
  net2cem_drops =============== 50/527658759
    net2cem_drops_underflow === 25
    net2cem_drops_overflow ==== 25
  Last cleared 6d02h
CEM0/2 errors:
  net2cem_drops =============== 2/526990836
    net2cem_drops_overflow ==== 2
  Last cleared never
CEM0/3 errors:
  net2cem_drops =============== 1/526982274
    net2cem_drops_overflow ==== 1
  Last cleared never
CEM0/4 errors:
  net2cem_drops =============== 51/527658758
    net2cem_drops_underflow === 26
    net2cem_drops_overflow ==== 25
  Last cleared 6d02h
CEM0/5 errors:
  net2cem_drops =============== 48/527660498
    net2cem_drops_underflow === 24
    net2cem_drops_overflow ==== 24
  Last cleared 6d02h

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

Related Commands

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

show connection

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

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

Syntax Description

all	(Optional) Displays information about all interworking connections.
element	(Optional) Displays information about the specified connection element.
id *ID*	(Optional) Displays information about the specified connection identifier.
name *name*	(Optional) Displays information about the specified connection name.
port *port*	(Optional) Displays information about all connections on an interface. (In Cisco IOS Release 12.0S, only ATM, serial, and Fast Ethernet connections are shown.)

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

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

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

Table A-1 describes the significant fields shown in the display.

Table A-1 show connection Field Descriptions

Field	Description
ID	Arbitrary connection identifier assigned by the operating system.
Name	Name of the connection.
Segment 1 Segment 2	Information about the interworking segments, including: • Interface name and number. • Segment state, interface name and number, and channel ID. Segment state displays nothing if the segment state is UP, "-" if the segment state is DOWN, and "***Card Removed***" if the segment state is DETACHED. • 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 similar 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.

show controller

Use the **show controller** command to display the status of an interface.

show controller {ATM | Async | BITS | CEM | E1 | GigabitEthernet | J1 | T1 | RTM} *slot* **/** *port*

Syntax Description

ATM	Displays the status of the ATM controller.
Async	Displays the status of the async controller.
BITS	Displays the status of the BITS controller.
CEM	Displays the status of the CEM controller.
E1	Displays the status oft the E1 controller.
GigabitEthernet	Displays the status of the Gigabit Ethernet controller.
J1	Displays the status of the J1 controller.
T1	Displays the status of the T1 controller.
RTM	Displays the status of the RTM controller.
slot	The slot number of the interface.
port	The port number of the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

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

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

Related Commands

Command	Description
show atm pvc	Displays the status of ATM PVCs and SVCs.
show frame-relay pvc	Displays the status of Frame Relay interfaces.

show gsm-abis efficiency

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

show gsm-abis efficiency [history]

Syntax Description

history	(Optional) Creates a graph display of the efficiency.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following examples show the output generated by this command:

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

Router# sh gsm eff history ser0/2:0

mwr1   04:00:00 PM Tuesday Apr 8 2008 est


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

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

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



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


mwr1   04:00:03 PM Tuesday Apr 8 2008 est


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

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

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis errors

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

show gsm-abis errors

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows the output generated by this command:

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

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

Table A-2 show gsm-abis errors Field Descriptions

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

Table A-2 show gsm-abis errors Field Descriptions (continued)

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis packets

To display packet statistics counters of GSM compression/decompression, use the **show gsm-abis packets** command in privileged EXEC mode. Include the **include retransmit** keyword to see the repetitive subrate 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(19)MR2	This command was incorporated.

Examples

The following **show gsm-abis packets** example shows the output generated by this command:

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

The following **show gsm-abis packets | include retransmit** example shows the output generated by this command:

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis peering

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

show gsm-abis peering [details]

Syntax Description

details	(Optional) Provides detailed information about peering.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following examples show the output generated by this command:

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

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

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

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

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

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

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

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

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

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show gsm-abis traffic

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

show gsm-abis traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows the output generated by this command:

```
Router# show gsm-abis traffic

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

Related Commands

Command	Description
clear gsm-abis	Clears the statistics displayed.

show interface switchport backup

Displays status information about the backup switchport.

show interface switchport backup [detail]

Syntax Description

detail	Provides additional information about the backup interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows the output generated by this command:

```
Router# show interface switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/0      GigabitEthernet0/5      Active Down/Backup Down
```

Related Commands

Command	Description
switchport backup interface	Configures a backup interface pair.

show ip rtp header-compression

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

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

Syntax Description

type number	(Optional) Interface type and number.
detail	(Optional) Displays details of each connection. **Note** This keyword is not supported on the Cisco MWR 2941-DC router. See "Usage Guidelines."

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

Examples

The following example shows output from the **show ip rtp header-compression** command:

```
Router# show ip rtp header-compression

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

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

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

Field	Description
Interface	Type and number of the interface.
Rcvd: total	Number of packets received on the interface.
compressed	Number of packets with compressed headers.

Table A-3 show ip rtp header-compression Field Descriptions (continued)

Field	Description
errors	Number of errors.
dropped	Number of dropped packets.
buffer copies	Not applicable to the Cisco MWR 2941-DC router.
buffer failures	Not applicable to the Cisco MWR 2941-DC router.
Sent: total	Total number of packets sent.
compressed	Number of packets sent with compressed headers.
bytes saved	Total savings in bytes as a result of compression.
bytes sent	Not applicable to the Cisco MWR 2941-DC router.
efficiency improvement factor	Efficiency achieved through compression.
Connect: rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
long searches	Not applicable to the Cisco MWR 2941-DC router.
misses	Number of new states that were created.
hit ratio	Number of times that existing states were revised.
five minute miss rate	Average miss rate.
max.	Maximum miss rate.
negative cache	Not applicable to the Cisco MWR 2941-DC router.

Related Commands

Command	Description
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 mpls l2transport vc

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

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

Syntax Description

vcid	(Optional) Allows you to enter a specific VC ID to display.
vc-id	(Optional) The VC ID number.
vc-id-min *vc-id-max*	(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.
name	(Optional) The name of the interface or subinterface.
local-circuit-id	(Optional) The number assigned to the local circuit. This argument value is supported only by the following transport types: • 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.
ip-address	(Optional) The IP address of the remote router.
name	(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
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

Examples

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

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

```
Router# show mpls l2transport vc
```

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

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

Table A-4 show mpls l2transport vc Field Descriptions

Field	Description
Local intf	The interface on the local router that has been enabled to transport Layer 2 packets.
Local circuit	The type and number (if applicable) of the local circuit. The output shown in this column varies, depending on the transport type: • 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.
Status	The status of the VC. The status can be one of the following conditions: • 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. – 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
Local interface	Interface on the local router that has been enabled to send and receive Layer 2 packets. The interface varies, depending on the transport type. The output also shows the status of the interface.
line protocol	Status of the line protocol on the edge-facing interface.
Destination address	IP address of the remote router specified for this VC. Specify the destination IP address as part of the **mpls l2transport route** command.
VC ID	VC identifier assigned to the interface on the router.
VC status	Status of the VC, which is one of the following conditions: 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. • 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.) DOWN—The VC is not ready to carry traffic between the two VC endpoints. ADMIN DOWN—The VC has been disabled by a user.
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	Status of the default path, which can be disabled or active. 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.
Create time	Time when the VC was provisioned.
last status change time	Last time the VC state changed.

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

Field	Description
Signaling protocol	Type of protocol used to send the MPLS labels. The output also shows the status of the peer router.
MPLS VC labels	Local VC label is a disposition label, which determines the egress interface of an arriving packet from the MPLS backbone. The remote VC label is a disposition VC label of the remote peer router.
Group ID	Local group ID is used to group VCs locally. The remote group ID is used by the peer to group several VCs.
MTU	Maximum transmission unit specified for the local and remote interfaces.
Remote interface description	Interface on the remote router that has been enabled to transmit and receive Layer 2 packets.
Tunnel label	An IGP label used to route the packet over the MPLS backbone to the destination router with the egress interface. The first part of the output displays the type of label. The second part of the output displays the route information. The tunnel label information can display any of the following states: • 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, label forwarding information base (LFIB) disabled—The MPLS switching subsystem is disabled. • not ready, 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.

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

Field	Description
packet totals	Number of packets sent and received. Received packets are those AToM packets received from the MPLS core. Sent packets are those AToM packets sent to the MPLS core. This number does not include dropped packets.
byte totals	Number of bytes sent and received from the core-facing interface, including the payload, control word if present, and AToM VC label.
packet drops	Number of dropped packets.

Related Commands

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

show network-clocks

To display information about the network clocks configured on the router, use the **show network-clocks** command. The command shows the priority and state of all configured clocks and the currently selected clock.

show network-clocks

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows how to use the set network-clock-select force-reselect command:

```
Router# show network-clocks
```

Related Commands

Command	Description
set network-clock-select force-reselect	This command causes the router to reselect a network clock.

show platform hardware

To display the status of hardware devices on the Cisco MWR 2941-DC, use the **show platform hardware** command. The command displays information about hardware devices on the Cisco MWR 2941-DC for troubleshooting and debugging purposes.

show platform hardware {adrian | bits | cpld | cpu | ethernet | fio | hwic | rtm | stratum | ufe winpath} [detail] [stats]

Syntax Description

adrian	Displays information about the adrian hardware.
bits	Displays information about the BITS hardware.
cpld	Displays information about the CPLD hardware.
cpu	Displays information about the CPU.
ethernet	Displays information about the ethernet interfaces on the Cisco MWR 2941-DC.
fio	Displays information about the FIO fpga hardware.
hwic	Displays information about the HWICs installed on the Cisco MWR 2941-DC.
rtm	Displays information about the RTM Module (ASM-M2900-TOP daughter card).
stratum	Displays information about the stratum hardware.
ufe	Displays information about the UFE hardware.
winpath	Displays information about the Winpath hardware.
detail	Display additional detail about Cisco MWR 2941-DC hardware.
stats	Displays RTM statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Related Commands

Command	Description
show controller	Displays the status of system controllers.

show ptp clock

Displays information about the PTP clock.

show ptp clock

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show ptp clock** command to display information about the PTP clock.

Examples

```
Router# show ptp clock
 PTP CLOCK INFO
  PTP Device Type: Ordinary clock
  Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E
  Clock Domain: 2
  Number of PTP ports: 1
  Priority1: 128
  Priority2: 128
  Clock Quality:
        Class: 13
        Accuracy: Within 1s
        Offset (log variance): 52592
  Offset From Master: 0
  Mean Path Delay: 0
  Steps Removed: 0
  Local clock time: 19:58:40 UTC Oct 30 2000
```

Related Commands

Command	Description
show ptp foreign-master-record	Displays the PTP foreign master records.
show ptp parent	Displays the PTP parent properties.
show ptp port	Displays the PTP port properties.
show ptp time-property	Displays the time properties of the PTP clock.

show ptp foreign-master-record

To display the PTP foreign master record set, use the **show ptp foreign-master-record** command in user EXEC mode.

show ptp foreign-master-record

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show ptp foreign-master-record** command to display the PTP foreign master records.

Examples

The following example shows output from the **show ptp foreign-master-record** command:

```
Router# show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface Vlan2
Number of foreign records 1, max foreign records 5
Best foreign record 0
RECORD #0
Foreign master port identity: clock id: 0x0:1E:4A:FF:FF:96:D2:A9
Foreign master port identity: port num: 1
Number of Announce messages: 8
Number of Current Announce messages: 6
Time stamps: 1233935406, 664274927
```

Related Commands

Command	Description
show ptp clock	Displays information about the PTP clock.
show ptp parent	Displays the PTP parent properties.
show ptp port	Displays the PTP port properties.
show ptp time-property	Displays the time properties of the PTP clock.

show ptp parent

To display the properties of the PTP parent, use the **show ptp parent** command in user EXEC mode.

show ptp parent

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show ptp parent** command to display the properties of the PTP parent.

Examples

The following example shows output from the **show ptp parent** command:

```
Router# show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E
  Parent Port Number: 0
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: 0

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:1E:4A:FF:FF:96:A9:9E
  Grandmaster Clock Quality:
        Class: 248
        Accuracy: Greater than 10s
        Offset (log variance): 52592
        Priority1: 128
        Priority2: 128
```

Related Commands

Command	Description
show ptp clock	Displays information about the PTP clock.
show ptp foreign-master-record	Displays the PTP foreign master records.
show ptp port	Displays the PTP port properties.
show ptp time-property	Displays the time properties of the PTP clock.

show ptp port

To display the PTP port properties, use the **show ptp port** command in user EXEC mode.

show ptp port

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show ptp port** command to o display the PTP port properties.

Examples

The following example shows output from the **show ptp port** command:

```
Router# show ptp port
PTP PORT DATASET: Vlan1
  Port identity: clock identity: 0x0:1E:4A:FF:FF:96:A9:9E
  Port identity: port number: 1
  PTP version: 2
  Delay request interval(log mean): 0
  Announce receipt time out: 0
  Peer mean path delay: 0
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 6000
```

Related Commands

Command	Description
show ptp clock	Displays information about the PTP clock.
show ptp foreign-master-record	Displays the PTP foreign master records.
show ptp parent	Displays the PTP parent properties.
show ptp time-property	Displays the time properties of the PTP clock.

show ptp time-property

To display the PTP clock time properties, use the **show ptp time-property** command in user EXEC mode.

show ptp time-property

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

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

Usage Guidelines

Use the **show ptp time-property** command to display PTP clock time properties.

Examples

The following example shows output from the **ptp time-property** command:

```
Router# show ptp time-property
 PTP CLOCK TIME PROPERTY
  Current UTC offset valid: 1
  Current UTC offset: 33
  Leap 59: 0
  Leap 61: 0
  Time Traceable: 0
  Frequency Traceable: 1
  PTP Timescale: 1
  Time Source: Hand Set
```

Related Commands

Command	Description
show ptp clock	Displays information about the PTP clock.
show ptp foreign-master-record	Displays the PTP foreign master records.
show ptp parent	Displays the PTP parent properties.
show ptp port	Displays the PTP port properties.

show xconnect all

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

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

Syntax Description

all	Displays information about all xconnect attachment circuits and PWs.
interface *interface*	Displays information about xconnect attachment circuits and PWs on the specified interface. Valid values for the argument are as follows: • **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 connect (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. • **gigabitethernet** *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** *vcid*}	Displays information about xconnect attachment circuits and PWs associated with the specified peer IP address. • **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
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

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

Examples

The following example shows **show xconnect all** command output in the brief (default) display format. The output shows information about the interfaces and VCs that have been configured to transport various Layer 2 packets on the router.

```
Router# show xconnect all

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST     Segment 1  S1 Segment 2 S2
ST     Segment 1                       S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Et0/0(Ethernet)             UP mpls 10.55.55.2:1000              UP
UP     ac   Et1/0.1:200(Eth VLAN)       UP mpls 10.55.55.2:5200              UP
IA pri ac   Et1/0.2:100(Eth VLAN)       UP ac   Et2/0.2:100(Eth VLAN)        UP
UP sec ac   Et1/0.2:100(Eth VLAN)       UP mpls 10.55.55.3:1101              UP
```

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

Table A-6 show xconnect all Field Descriptions

Field	Description
XC ST	• 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.
Segment 1 or Segment 2	Information about the type of xconnect, the interface type, and the IP address the segment is using. Types of xconnects are: • ac—Attachment circuit. • pri ac—Primary attachment circuit. • sec ac—Secondary attachment circuit. • mpls—Multiprotocol Label Switching. • l2tp—Layer 2 Tunnel Protocol.
S1 or S2	State of the segment. Valid states are: • 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)              UP mpls 10.55.55.2:1000              UP
            Interworking: ip                    Local VC label 16
                                                Remote VC label 16
                                                pw-class: mpls-ip
UP     ac   Et1/0.1:200(Eth VLAN)        UP mpls 10.55.55.2:5200              UP
            Interworking: ip                    Local VC label 17
                                                Remote VC label 20
                                                pw-class: mpls-ip
IA pri ac   Et1/0.2:100(Eth VLAN)        UP ac   Et2/0.2:100(Eth VLAN)        UP
            Interworking: none                  Interworking: none
UP sec ac   Et1/0.2:100(Eth VLAN)        UP mpls 10.55.55.3:1101              UP
            Interworking: none                  Local VC label 23
                                                Remote VC label 17
                                                pw-class: mpls
```

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

snmp-server enable traps ipran

no snmp-server enable traps ipran

Related Commands This command has no arguments or keywords.

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

Command Modes Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples The following example shows the output generated by this command:

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

Related Commands

Command	Description
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 alarm-gsm

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

snmp-server enable traps ipran alarm-gsm

no snmp-server enable traps ipran alarm-gsm

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

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows the output generated by this command:

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

Related Commands

Command	Description
snmp-server enable traps ipran util	Provides information on backhaul utilization.
snmp-server enable traps ipran	Enables all notifications.

snmp-server enable traps ipran util

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

snmp-server enable traps ipran util

no snmp-server enable traps ipran util

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows 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	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.

switchport backup interface

Use the **switchport backup interface** interface configuration command on a Layer 2 interface to configure Flex Links, a pair of interfaces that provide backup to each other. Use the **no** form of this command to remove the Flex Links configuration.

switchport backup interface {*interface-id***} preemption {delay** *delay-time* **| mode {bandwidth | forced | off}}**

no switchport backup interface {*interface-id***} preemption {delay** *delay-time* **| mode {bandwidth | forced | off}}**

Syntax Description

interface-id	The Layer 2 interface that acts as a backup link to the interface being configured. The interface can be a physical interface or port channel. The port-channel range is 1–486.
preemption	Configures a preemption scheme for a backup interface pair.
delay	(Optional) Specifies a preemption delay.
delay-time	(Optional) Specifies the length of the preemption delay; valid values are 1–300 seconds.
mode	Specifies the preemption mode as bandwidth, forced, or off.
bandwidth	(Optional) Specifies that the interface with the higher available bandwidth always preempts the backup.
forced	(Optional) Specifies that the interface always preempts the backup.
off	(Optional) Specifies that no preemption occurs from backup to active.

Defaults

There is no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Examples

The following example shows the output generated by this command:

```
Router(config)# interface gigabitethernet0/3
Router(config-if)# switchport backup interface gigabitethernet0/4
```

Related Commands

Command	Description
show interface switchport backup	Displays status information about the backup switchport.

xconnect

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

xconnect *peer-ip-address* | *vcid* | *pseudowire-parameters* [**ignore-vpi-vci**]

no xconnect

Syntax Description

peer-ip-address	IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.
vcid	The 32-bit identifier of the virtual circuit (VC) between the PE routers.
pseudowire-parameters	Encapsulation and pseudowire-class parameters to be used for the attachment circuit. At least one of the following PW parameters must be configured: • **encapsulation** {**l2tpv3** | **mpls**}— Specifies the tunneling method to encapsulate the data in the PW: – **l2tpv3**—Specifies L2TPv3 as the tunneling method. – **mpls**—Specifies MPLS as the tunneling method. **Note** L2TP is not currently supported on the Cisco MWR 2941-DC. • **pw-class** *pw-class-name*—Specifies the pseudowire-class configuration from which the data encapsulation type is taken. This option is mandatory if you select an encapsulation method.
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	Applies only when the **xconnect** command is configured under the AAL0 encapsulation PVC. The keyword specifies the PW type as a one-to-one VCC cell relay.
ignore-vpi-vci	This parameter sets the Cisco MWR 2941-DC to ignore the VPI/VCI value in the PW packet and rewrite the egress ATM cell header with VPI/VCI value of the locally configured (attachment side) PVC. **Note** You can only use this parameter for a 1-to-1 pseudowire, for which you apply the xconnect command to a PVC.

Defaults

The attachment circuit is not bound to the PW.

Command Modes

CEM circuit configuration

Interface configuration

Subinterface configuration

l2transport configuration (for ATM)

Connect configuration

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

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

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

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

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

ignore-vpi-vci Keyword

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

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

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

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

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

Examples

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

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

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

MWR:

```
Router# config t
Router(config)# interface ATM 0/0
Router(config-if)# pvc 0/10 12transport
Router(config-if-atm-l2trans-pvc)# encapsulation aa10
Router(config-if-atm-l2trans-pvc)# xconnect 10.10.10.10 100 encapsulation mpls ignore-vpi-vci
Router(config-if-atm-l2trans-pvc-xconn)# exit
Router(config-if-atm-l2trans-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 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aa10
Router(config-if-atm-l2trans-pvc)# xconnect 20.20.20.20 100 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
pseudowire-class	Configures a template of PW configuration settings used by the attachment circuits transported over a PW.
show xconnect	Displays information about xconnect attachment circuits and PWs.

xconnect logging redundancy

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

xconnect logging redundancy

no xconnect logging redundancy

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.4(19)MR2	This command was incorporated.

Usage Guidelines

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

Examples

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

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

Activating the Primary Member

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

Activating the Backup Member:

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

Related Commands

Command	Description
xconnect	Binds an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to an Layer 2 PW for xconnect service and enters xconnect configuration mode.