

loopback T1 interface through nrzi-encoding

- loopback (T1 interface), on page 3
- loopback (T3/E3 controller), on page 6
- loopback (T3-E3 interface), on page 8
- loopback applique, on page 10
- loopback dte, on page 11
- loopback line, on page 12
- loopback remote (interface), on page 14
- loopback remote (T1/T3/SDH/SONET Controller), on page 17
- loopback (SONET), on page 20
- mac-address-table learning, on page 21
- mac-address (virtual switch), on page 23
- mac-address-table secure, on page 25
- main-fiber port, on page 29
- max-reserved-bandwidth, on page 30
- mdix auto, on page 33
- mdl, on page 34
- media-type, on page 36
- media-type auto-failover, on page 38
- member subslot, on page 39
- microcode reload controller, on page 43
- mls exclude protocol, on page 44
- mls ip delete-threshold, on page 45
- mls ip directed-broadcast, on page 46
- mls ipx, on page 48
- mls verify, on page 49
- mobility, on page 51
- mode, on page 53
- mode (ATM T1 E1 controller), on page 56
- mode (HSA redundancy), on page 59
- mode (RSC redundancy), on page 61
- mode (T1 E1 controller), on page 62
- mode bypass, on page 65
- mode c-12, on page 67

- mode ct3, on page 69
- mode download, on page 70
- mode e3, on page 71
- mode sonet, on page 72
- mode sts-nc, on page 73
- mode t3/e3, on page 74
- mode two-way, on page 75
- mode vc-1x, on page 76
- mode vc-4, on page 77
- mode vc4-Nc, on page 78
- mode vt-15, on page 79
- mode t3, on page 80
- mode tug-3, on page 81
- modem dtr-delay, on page 82
- monitoring, on page 83
- mop enabled, on page 85
- mop sysid, on page 86
- mtu, on page 87
- national bit (controller), on page 90
- national bit (interface), on page 91
- national reserve, on page 92
- negotiation, on page 93
- neighbor (VPLS), on page 95
- network-clock (BITS), on page 97
- network-clock clear lockout, on page 100
- network-clock hold-off global, on page 102
- network-clock input-source, on page 103
- network-clock set lockout, on page 104
- network-clock synchronization ssm option, on page 106
- network-clock synchronization automatic, on page 108
- network-clock synchronization mode QL-enabled, on page 109
- network-clock quality-level, on page 110
- no channelized, on page 113
- nrzi-encoding, on page 115

loopback (T1 interface)

To loop individual T1 channels on the CT3IP in Cisco 7000 series routers that have the RSP7000 and RSP7000CI and in Cisco 7500 series routers, use the **loopback**command in interface configuration mode. To remove the loopback, use the **no** form of this command.

loopback [**local** | **network** {**line** | **payload**} | **remote** {**line** {**fdl** {**ansi** | **bellcore**} | **inband**} | **payload** [**fdl**] [**ansi**]}]
no loopback

Syntax Description

local	(Optional) Loops the router output data back toward the router at the T1 framer and sends an alarm indication signal (AIS) signal out toward the network.
network line | **payload**	(Optional) Loops the data back toward the network before the T1 framer and automatically sets a local loopback at the High-Level Data Link Control (HDLC) controllers (line), or loops the payload data back toward the network at the T1 framer and automatically sets a local loopback at the HDLC controllers (payload).
remote linefdl {**ansi**|**bellcore**	(Optional) Sends a repeating, 16-bit Extended Superframe (ESF) data link code word (00001110 11111111 for FDL ANSI and 00010010 11111111 for FDL Bellcore) to the remote end requesting that it enter into a network line loopback. Specify the **ansi** keyword to enable the remote line Facility Data Link (FDL) ANSI bit loopback on the T1 channel, per the ANSI T1.403 specification. Specify the **bellcore** keyword to enable the remote SmartJack loopback on the T1 channel, per the TR-TSY-000312 specification.
remote line inband	(Optional) Sends a repeating, 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback.
remote payload [**fdl**] [**ansi**]	(Optional) Sends a repeating, 16-bit ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 channel. You can optionally specify **fdl** and **ansi**, but it is not necessary.

Command Default

No loopback is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command for troubleshooting purposes.

To better diagnose T1 provisioning problems, you can place the remote CSU or remote SmartJack into loopback. The **loopbackremotelinefdl** interface configuration command allows you to place either the CSU or the SmartJack into loopback:

- **ansi** --Places the CSU into loopback, per the ANSI T1.403 Specification.
- **bellcore** --Places the SmartJack into loopback, per the TR-TSY-000312 Specification.

When both are configured, transmission of loss of frame (LOF) indication (yellow alarm) takes priority over transmission of some facilities data link (FDL) messages.

If the remote loopback appears not to be working, use the show controllers t3 command to determine if the given T1 is currently attempting to transmit a LOF indication (yellow alarm):

```
Router#
show controllers t3 0/0/0:2
T3 0/0/0 is up.
   CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.5.9
   Mx H/W version: 2, Mx ucode ver: 1.34

   T1 2 is down, speed: 1536 kbs, non-inverted data
   timeslots: 1-24
   FDL per AT&T 54016 spec.
   Transmitter is sending LOF Indication.
   Receiver is getting AIS.
```

If the transmitter is sending a LOF indication, as in the previous example, stop the transmission of the LOF indication (yellow alarm) with the no t1 yellow generation configuration command as shown in the following example:

```
Router(config)# controllers t3 0/0/0
Router(config-controller)# no t1 2 yellow generation
Router(config-controller)# Ctrl-D
```

To verify that the transmission of the LOF indication (yellow alarm) has stopped, use the show controllers t3 command:

```
Router# show controllers t3 0/0/0:2
T3 0/0/0 is up.
   CT3 H/W Version: 5, CT3 ROM Version: 1.2, CT3 F/W Version: 2.5.9
   Mx H/W version: 2, Mx ucode ver: 1.34
   T1 2 is down, speed: 1536 kbs, non-inverted data
   timeslots: 1-24
   FDL per AT&T 54016 spec.
   Receiver is getting AIS.
   Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
   Yellow Alarm Generation is disabled
```

Then retry the remote loopback command. When diagnosis is complete, remember to reenable the LOF indication (yellow alarm).

You can also loopback all the T1 channels by using the**loopback**(CT3IP) interface configuration command.

Examples

The following example configures T1 channel 5 for a local loopback:

```
Router(config)# interface serial 3/0/0:5
Router(config-if)# loopback local
```

Related Commands

Command	Description
loopback (T3 controller)	Loops the entire T3 (all 28 T1 channels) on the CT3IP in Cisco 7500 series routers.
t1 yellow generation	Enables detection and generation of yellow alarms for a T1 channel on the CT3IP in Cisco 7500 series routers.

loopback (T3/E3 controller)

To loop the entire T3 (all 28 T1 channels) line on the T3 controller or E3 (all 16 E1 channels) in Cisco NCS 4200 Series or on the CT3IP in Cisco 7500 series routers, use the **loopback** command in controller configuration mode. To remove the loop, use the **no** form of this command.

loopback {**local** | **network** {**line** | **payload**} | **remote**}
no loopback

Syntax Description

local	Loops the data back toward the router and sends an alarm indication signal (AIS) out toward the network.
network line payload	Sets the loopback toward the network either before going through the framer (line) or after going through the framer (payload).
remote	Sends a far-end alarm control (FEAC) request to the remote end requesting that it enter into a network line loopback. FEAC requests (and therefore remote loopbacks) are possible only when the T3 is configured for C-bit framing. The M23 format does not support remote loopbacks.

Command Default

No loops are configured on the T3/E3 line.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for T3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

Use this command for troubleshooting purposes. To verify that a loopback is configured on the interface, use the **showcontrollersT3/E3**EXEC command. Note that remote loopback is available only in C-bit parity mode.

You can also loopback each T1/E1 channel by using the**loopback** interface configuration command for T1/E1.

For more information, refer to the “Troubleshooting the T3 and T1 Channels” section in the “Configuring Serial Interfaces” chapter of the *CiscoIOSInterfaceandHardwareComponentConfigurationGuide*.

Examples

The following example configures the T3/E3 or CT3IP for a local loopback:

```
Router(config)# controller t3/e3 3/0/0
Router(config-controller)# loopback local
```

Related Commands

Command	Description
framing	Selects the frame type for the T1 or E1 data line.
loopback (interface)	Places the specified module in loopback mode.
loopback remote (interface)	Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back.
show controllers t3/e3	Displays information about the T3/E3 controllers.

loopback (T3-E3 interface)

To loopback at various points in the transmit and receive path, use the **loopback**command in interface configuration mode. To stop the loopback, use the no form of this command.

PA-T3 Port Adapter
loopback {**dte** | **local** | **network** {**line** | **payload**} | **remote**}
no loopback

PA-E3 Port Adapter
loopback {**dte** | **local** | **network** {**line** | **payload**}}
no loopback

T3/E3 Shared Port Adapters
loopback {**dte** | **local** | **dual** | **network** {**line** | **payload**} | **remote**}
no loopback {**dte** | **local** | **dual** | **network** {**line** | **payload**} | **remote**}

Syntax Description

dte	Loopback after the line interface unit (LIU) towards the terminal.
local	Loopback after going through the framer toward the terminal.
dual	Sets both local loopback and network line loopback. The dual keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Channelized T3 SPA.
network **line** | **payload**	Sets the loopback toward the network before going through the framer (**line**) or after going through the framer (**payload**).
remote	Sends FEAC to set remote in loopback.

Command Default

No loopback by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for E3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.

Release	Modification
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches. The **dual** keyword was added.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the loopback command to diagnose problems on the local port, between the framer and the line interface unit (LIU) level.

To verify that a loopback is configured on the interface, use the **showinterfacesserial** or **showinterfacesloopback** command.

The dual keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Channelized T3 SPA.

Examples

The following example configures the serial interface located in slot 3/0/0 for a local loopback:

```
Router(config)# interface serial 3/0/0
Router(config-if)# loopback local
```

The following example creates a loopback on slot 5, bay 0 after the LIU towards the terminal.

```
Router# configure terminal
Router(config)# interface serial 5/0/0
Router(config-if)# loopback dte
```

Related Commands

Command	Description
show controllers serial	Displays information that is specific to the interface hardware.
show interfaces loopback	Displays information about the loopback interface.
show interfaces serial	Displays information about a serial interface.

loopback applique

To configure an internal loop on the High-Speed Serial Interface (HSSI) applique, use the **loopbackapplique** command in interface configuration mode. To remove the loop, use the **no** form of this command.

loopback applique commandloopback applique
no loopback applique

Syntax Description

This command has no arguments or keywords.

Command Default

No loops are configured on the HSSI applique.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command loops the packets within the applique to provide a way to test communication within the router or access server. It is useful for sending pings to yourself to check functionality of the applique.

To show a specific interface that is currently in loopback operation, use the **showinterfacesloopback** EXEC command.

Examples

The following example configures the loopback test on the HSSI applique:

```
Router(config)# interface serial 1
Router(config-if)# loopback applique
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback dte

To loop packets back to the DTE from the CSU/DSU, when the device supports this function, use the **loopbackdte**command in interface configuration mode. To remove the loop, use the **no** form of this command.

loopback dte commandloopback dte
no loopback dte

Syntax Description

This command has no arguments or keywords.

Command Default

No loops are configured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is useful for testing the DTE-to-DCE cable.

This command is used to test the performance of the integrated CSU/DSU. Packets are looped from within the CSU/DSU back to the serial interface of the router. Send a test ping to see if the packets successfully looped back. To cancel the loopback test, use the **noloopbackdte** command.

When using the 4-wire 56/64-kbps CSU/DSU module, an out-of-service signal is transmitted to the remote CSU/DSU.

To show a specific interface that is currently in loopback operation, use the**showinterfacesloopback** EXEC command.

Examples

The following example configures the loopback test on the DTE interface:

```
Router(config)# interface serial 0
Router(config-if)# loopback dte
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.

loopback line

To loop packets completely through the CSU/DSU to configure the CSU loop, use the **loopbackline** command in interface configuration mode. To remove the loop, use the **no** form of this command.

loopback line [**payload**]
no loopback line [**payload**]

Syntax Description

payload	(Optional) Configures a loopback point at the DSU and loops data back to the network on an integrated CSU/DSU.

Command Default

No loops are configured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is useful for testing the DCE device (CSU/DSU) itself. When the **loopbackline** command is configured on the 2-wire 56-kbps CSU/DSU module or the 4-wire 56/64-kbps CSU/DSU modules, the network data loops back at the CSU and the router data loops back at the DSU. If the CSU/DSU is configured for switched mode, you must have an established connection to perform a payload-line loopback. To loop the received data through the minimum amount of CSU/DSU circuitry, issue the **loopbackline** command.

When you issue the **loopbacklinepayload** command on an integrated CSU/DSU module, the router cannot transmit data through the serial interface for the duration of the loopback. Choosing the DSU as a loopback point loops the received-network data through the maximum amount of CSU/DSU circuitry. Data is not looped back to the serial interface. An active connection is required when operating in switched mode for payload loopbacks.

If you enable the **loopbackline** command on the fractional T1/T1 module, the CSU/DSU performs a full-bandwidth loopback through the CSU portion of the module and data transmission through the serial interface is interrupted for the duration of the loopback. No reframing or corrections of bipolar violation errors or cyclic redundancy check (CRC) errors are performed. When you configure the **loopbacklinepayload**command on the FT1/T1 module, the CSU/DSU performs a loopback through the DSU portion of the module. The **loopbacklinepayload**command reframes the data link, regenerates the signal, and corrects bipolar violations and Extended Super Frame CRC errors.

When performing a T1-line loopback with Extended Super Frame, communication over the facilities data link is interrupted, but performance statistics are still updated. To show interfaces currently in loopback operation, use the **showservice-module**EXEC command.

To show interfaces that are currently in loopback operation on other routers, use the **showinterfacesloopback** EXEC command.

Examples

The following example configures the loopback test on the DCE device:

```
Router(config)# interface serial 1
Router(config-if)# loopback line
```

The following example shows how to configure a payload loopback on a Cisco 2524 or Cisco 2525 router:

```
Router1(config-if)# loopback line payload
Loopback in progress
Router1(config-if)# no loopback line
```

The following example shows the output on a Cisco 2524 or Cisco 2525 router when you loop a packet in switched mode without an active connection:

```
Router1(config-if)# service-module 56k network-type switched
Router1(config-if)# loopback line payload
Need active connection for this type of loopback
% Service module configuration command failed: WRONG FORMAT.
```

Related Commands

Command	Description
show interfaces loopback	Displays information about the loopback interface.
show service-module	Displays the performance report for an integrated CSU/DSU.

loopback remote (interface)

To loop packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back, use the **loopbackremote**command in interface configuration mode. To remove the loopback, use the **no** form of this command.

FT1/T1 CSU/DSU Modules
loopback remote {**full** | **payload** | **smart-jack**} [**0in1** | **1in1** | **1in2** | **1in5** | **1in8** | **3in24** | **qrw** | **user-pattern** *24-bit-binary-value*]
no loopback remote {**full** | **payload** | **smart-jack**}

2- and 4-Wire, 56/64-kbps CSU/DSU Modules
loopback remote [**2047** | **511** | **stress-pattern** *pattern-number*]
no loopback remote

Syntax Description

full	Transmits a full-bandwidth line loopback request to a remote device, which is used for testing.
payload	Transmits a payload line loopback request to a remote device, which is used for testing the line and remote DSU.
smart-jack	Transmits a loopback request to the remote smart jack, which some service providers attach on the line before the customer premises equipment (CPE). You cannot put the local smart jack into loopback.
0in1	(Optional) Transmits an all-zeros test pattern used for verifying B8ZS line encoding. The remote end might report a loss of signal when using alternate mark inversion (AMI) line coding.
1in1	(Optional) Transmits an all-ones test pattern used for signal power measurements.
1in2	(Optional) Transmits an alternating ones-and-zeroes test pattern used for testing bridge taps.
1in5	(Optional) Transmits the industry-standard test-pattern loopback request.
1in8	(Optional) Transmits a test pattern used for stressing timing recovery of repeaters.
3in24	(Optional) Transmits a test pattern used for testing the ones density tolerance on AMI lines.
qrw	(Optional) Transmits a quasi-random word test pattern, which is a random signal that simulates user data.
user-pattern *24-bit-binary-value*	(Optional) Transmits a test pattern that you define. Enter a binary string up to 24 bits long. For the fixed patterns such **0in1** and **1in1**, the T1 framing bits are jammed on top of the test pattern; for the **user-pattern**, the pattern is simply repeated in the time slots.
2047	(Optional) Transmits a pseudorandom test pattern that repeats after 2047 bits.
511	(Optional) Transmits a pseudo random test pattern that repeats after 511 bits.

stress-pattern *pattern-number*	(Optional) Transmits a DDS stress pattern available only on the 4-wire 56/64-kbps CSU/DSU module. You may enter a stress pattern from 1 to 4. A 1 pattern sends 100 bytes of all 1s and then 100 bytes of all 0s to test the stress clocking of the network. A 2 pattern sends 100 bytes of a 0x7e pattern and then 100 bytes of all 0s. A 3 pattern sends continuous bytes of a 0x46 pattern. A 4 pattern sends continuous bytes of a 0x02 pattern.

Command Default

No remote loopback interface is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used for testing the data communication channels along with or without remote CSU/DSU circuitry. The loopback is usually performed at the line port, rather than the DTE port, of the remote CSU/DSU.

For a multiport interface processor connected to a network via a channelized T1 link, the **loopbackremote** interface configuration command applies if the remote interface is served by a DDS line (56 kbps or 64 kbps) and if the device at the remote end is a CSU/DSU. In addition, the CSU/DSU at the remote end *must* react to latched DDS CSU loopback codes. Destinations that are served by other types of lines or that have CSU/DSUs that do not react to latched DDS CSU codes cannot participate in an interface remote loopback. Latched DDS CSU loopback code requirements are described in AT&T specification TR-TSY-000476, “OTGR Network Maintenance Access and Testing.”

For the integrated FT1/T1 CSU/DSU module, the **loopbackremotefull** command sends the loopup code to the remote CSU/DSU. The remote CSU/DSU performs a full-bandwidth loopback through the CSU portion of the module. The**loopbackremotepayload** command sends the loopup code on the configured time slots, while maintaining the D4-extended super frame. The remote CSU/DSU performs the equivalent of a loopback line payload request. The remote CSU/DSU loops back only those time slots that are configured on the remote end. This loopback reframes the data link, regenerates the signal, and corrects bipolar violations and extended super frame CRC errors. The **loopbackremotesmart-jack**command sends a loopup code to the remote smart jack. You cannot put the local smart jack into loopback.

Failure to loopup or initiate a remote loopback request could be caused by enabling the **noservice-modulet1remote-loopback** command or having an alternate remote-loopback code configured on the remote end. When the loopback is terminated, the result of the pattern test is displayed.

For the 2- and 4-wire, 56/64-kbps CSU/DSU module, an active connection is required before a loopup can be initiated while in switched mode. When transmitting V.54 loopbacks, the loopback mode is initiated on the remote device using V.54 messages. Failure to loopup or initiate a remote loopback request could be caused by enabling the **noservice-module56kremote-loopback** command.

To display interfaces that are currently in loopback operation, use the **showinterfacesloopback** EXEC command.

Examples

Example for Remote Loopback Test

The following example configures a remote loopback test:

```
Router(config)# interface serial 0

Router(config-if)# loopback remote
```

Example of Full-Bandwidth Line Loopback

The following example configures the remote device into full-bandwidth line loopback while specifying the **qrw** test pattern over the T1 CSU/DSU module on a Cisco 2524 or Cisco 2525 router:

```
Router(config)# interface serial 0
Router(config-if)# loopback remote full qrw
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down
%LINK-3-UPDOWN: Interface Serial0, changed state to down
%SERVICE_MODULE-5-LOOPUPREMOTE: Unit 0 - Remote unit placed in loopback
```

Example of Loopback Stress Pattern

The following example transmits a remote loopback stress pattern over the 4-wire, 56/64-kbps CSU/DSU module, which tests the stress clocking of the network:

```
Router(config-if)# loopback remote stress-pattern 1
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state to down
%LINK-3-UPDOWN: Interface Serial1, changed state to down
%SERVICE_MODULE-5-LOOPUPREMOTE: Unit 1 - Remote unit placed in loopback
```

Related Commands

Command	Description
clear service-module serial	Resets an integrated CSU/DSU.
loopback dte	Loops packets back to the DTE device from the CSU/DSU.
loopback line	Loops packets completely through the CSU/DSU to configure the CSU loop.
service-module 56k remote-loopback	Enables the acceptance of a remote loopback request on a serial interface on a 2- or 4-wire, 56/64-kbps CSU/DSU module.
service-module t1 remote-loopback	Specifies whether the fractional T1/T1 CSU/DSU module enters loopback mode when it receives a loopback code on the line.
show interfaces loopback	Displays information about the loopback interface.
show service-module serial	Displays the performance report for an integrated CSU/DSU.

loopback remote (T1/T3/SDH/SONET Controller)

To put the far-end T1 or T3 interfaces into a loopback use the **loopback remote** command in the global configuration mode.The remote loopback setting loops back the far-end at line or payload, using inband bit-orientated CDE (IBOC) or the extended super frame (ESF) loopback codes to communicate the request to the far-end.

T1 Controller
loopback remote {esf | {line {csu} | payload} iboc {fac1 | fac2 | csu}}

T3 Controller
loopback remote {line | payload}

Syntax Description

esf line csu	Remote line CSU loopback through FDL. This is the default option.
esf payload	Remote payload loopback through FDL.
iboc fac1	Remote inband line facility1 loopback.
iboc fac2	Remote inband line facility2 loopback.
iboc csu	Remote inband line CSU loopback.

Command Default

Loopback remote is disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Loopback testing is one of the troubleshooting methods which is an effective way to isolate the failing links. When the loopback is configured, all the data sent is received back. If the same data is not received then it is declared as link failure. In the similar way, remote loopback is configured to troubleshoot the link failure between two nodes.

Examples

The following example shows how to set T1 loopback remote iboc fac1 for DS1:

```
Router(config)# controller t1 0/0/1
Router(config-controller)#loopback remote iboc fac1
exit
```

The following example shows how to set T3 loopback remote line for DS3:

```
Router(config)# controller t3 0/0/1
Router(config-controller)#loopback remote line
exit
```

The following example shows how to set T3 loopback remote payload for OCX in sonet:

```
Router(config)# controller sonet 0/0/1
Router(config-controller)#sts 1
Router(config-ctrlr-sts1)#mode t3
Router(config-ctrlr-sts1)#t3 loopback remote payload
```

The following example shows how to set T1 loopback remote esf line csu for OCX in SDH:

```
Router(config)#controller sdh 0/4/7
Router(config-controller)#au-4 1
Router(config-ctrlr-tug3)#tug-3 3
Router(config-ctrlr-tug3)#mode vc1x
Router(config-ctrlr-tug3)#tug-2 1 payload vc11
Router(config-ctrlr-tug2-vcx)#t1 1 loopback remote esf line csu
```

Related Commands

Commands	URL
card type	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2336574570
cem-group	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2440628600
payload-size dejitter-buffer	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp3946673156
class cem	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2169323859
controller t1/e1	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp1472647421
xconnect	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-t2.html#wp8578094790
linecode	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-l1.html#wp2312535965
framing	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp2853515177
clock source	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp6081785140

Commands	URL
cable length	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp2492964151
bert pattern	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-a1.html#wp3620978929
channelized	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c1.html#wp7026926390
loopback	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-l1.html#wp1033903426
show controller t1	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s3.html#wp2149471094
show controller e1	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s2.html#wp1632676058

loopback (SONET)

To set the loopback method for testing an interface, use the **loopback** command in the controller configuration mode. To reset to the default, use the **no** form of this command.

loopback [*local* | *network* {*line* | *payload*}]

Syntax Description

local	The name of a CEM interface parameters class.
network {*line* | *payload*	Sets the loopback toward the network before going through the framer (*line*) or after going through the framer (*payload*).

Command Default

No loopback is configured.

Command Modes

Controller configuration

Command History

Release	Modification
3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

You can use a loopback test on lines to detect and distinguish equipment malfunctions caused by the line. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem.

Examples

The following example shows the configuration of VT 1.5-T1 loopback :

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
loopback local
sts-1 1
mode ct3
vtg 1 t1 1 loopback line
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

mac-address-table learning

To enable MAC-address learning, use the **mac-address-tablelearning**command in global configuration mode. To disable learning, use the **no** form of this command.

`mac-address-table learning` {`vlan`*vlan-id* | `interface`*interface slot/port*} {`module`[*module num*]}

`no mac-address-table learning` {`vlan`*vlan-id* | `interface`*interface slot/port*} {`module`[*module num*]}

Syntax Description

default	(Optional) Returns to the default settings.
vlan *vlan-id*	Specifies the VLAN to apply the per-VLAN learning of all MAC addresses; valid values are from 1 to 4094.
interface	Specifies per-interface based learning of all MAC addresses.
interface slot / port	Interface type, the slot number, and the port number.
module *num*	(Optional) Specifies the module number.

Command Default

If you configure a VLAN on a port in a module, all the supervisor engines and Distributed Forwarding Cards (DFCs) in the Cisco 7600 series router are enabled to learn all the MAC addresses on the specified VLAN.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can use the **module***num* keyword and argument to specify supervisor engines or DFCs only.

You can use the **vlan***vlan-id* keyword and argument on switch-port VLANs only. You cannot use the **vlan***vlan-id* keyword and argument to configure learning on routed interfaces.

You can use the **interface***interfaceslot/port* keyword and arguments on routed interfaces, supervisor engines, and DFCs only. You cannot use the **interface***interfaceslot/port* keyword and arguments to configure learning on switch-port interfaces or non-DFC modules.

Examples

This example shows how to enable MAC-address learning on a switch-port interface on all modules:

```
Router(config)# mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a switch-port interface on a specified module:

```
Router(config)# mac-address-table learning vlan 100 module 4
Router(config)#
```

This example shows how to disable MAC-address learning on a specified switch-port interface for all modules:

```
Router(config)# no mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a routed interface on all modules:

```
Router(config)# mac-address-table learning vlan 100
Router(config)#
```

This example shows how to enable MAC-address learning on a routed interface for a specific module:

```
Router(config)# mac-address-table learning interface FastEthernet 3/48 module 4
Router(config)#
```

This example shows how to disable MAC-address learning for all modules on a specific routed interface:

```
Router(config)# no mac-address-table learning interface FastEthernet 3/48
Router(config)#
```

Related Commands

Command	Description
show mac-address-table learning	Displays the MAC-address learning state.

mac-address (virtual switch)

To specify a Media Access Control (MAC) address to use as the common router MAC address for interfaces on the active and standby chassis, use the **mac-address** virtual switch configuration submode command. To return to the default setting, use the **no** form of this command.

mac-address {*mac-address* | **use-virtual**}

Syntax Description

mac-address	MAC address in hexadecimal format.
use-virtual	Specifies the MAC address range reserved for the virtual switch system (VSS).

Command Default

The router MAC address is derived from the backplane of the active chassis.

Command Modes

Virtual switch configuration submode (config-vs-domain)

Command History

Release	Modification
12.2(33)SXH2	Support for this command was introduced.

Usage Guidelines

When a virtual switch comes up, the router MAC address is derived from the backplane of the active chassis and is used as the common router MAC address for interfaces on both the active and the standby chassis. Between switchovers, this MAC address is maintained on the new active switch. You can enter the **mac-address***mac-address*command to specify a MAC address to use or the **mac-address**use-virtual to use the MAC address range reserved for the VSS.

The MAC address range reserved for the VSS is derived from a reserved pool of addresses with the domain ID encoded in the leading 6 bits of the last octet and trailing 2 bits of the previous octet of the mac-address. The last two bits of the first octet is allocated for protocol mac-address which is derived by adding the protocol ID (0 to 3) to the router MAC address.

Note You must reload the virtual switch for the new router MAC address to take effect. If the MAC address you configured is different from the current MAC address, the following message is displayed: Configured Router mac address is different from operational value. Change will take effect after config is saved and switch is reloaded.

Examples

The following example shows how to specify the MAC address to use in hexadecimal format:

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address 0000.0000.0000
Router(config-vs-domain)#
```

The following example shows how to specify the MAC address range reserved for the VSS:

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address use-virtual
Router(config-vs-domain)#
```

Related Commands

Command	Description
switch virtual domain	Assigns a switch number and enters virtual switch domain configuration submode.

mac-address-table secure

To add secure addresses to the MAC address table, use the **mac-address-tablesecure** command in global configuration mode. To remove secure entries from the MAC address table, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

no mac-address-table secure *hw-address* **vlan** *vlan-id*

Catalyst Switches

mac-address-table secure *hw-address* [**atm** *slot/port***vlan** *vlan-id*]
no mac-address-table secure *hw-address* [**vlan** *vlan-id*]

Cisco 860 Series Integrated Services Routers (ISRs) and Cisco 880 Series ISRs

mac-address-table secure [**H.H.H** | **maximum** *maximum addresses*]
no mac-address-table secure [**H.H.H** | **maximum** *maximum addresses*]

Syntax Description

hw -address	MAC address that is added to the table.
interface	Port to which packets destined for *hw-address* are forwarded.
fa	Specifies FastEthernet.
gi	Specifies Gigabit Ethernet.
H.H.H	(Optional) Specifies 48-bit hardware address.
slot	(Optional) The slot (slot 1 or slot 2) to which to add dynamic addresses.
port	(Optional) Port interface number. The ranges are based on type of Ethernet switch network module used: • 0 to 15 for NM-16ESW • 0 to 35 for NM-36ESW • 0 to 1 for GigabitEthernet
atm *slot* / *port*	(Optional) Add secure addresses to the ATM module in slot 1 or 2. The port is always 0 for an ATM interface.
maximum *maximum addresses*	(Optional) Applies only to Cisco 860 series and Cisco 880 series ISRs. Range is 1-200.

vlan *vlan -id*	Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports. The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes. Catalyst Switches (Optional) The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-address* are forwarded. The **vlan** keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address. This keyword is required for multi-VLAN and trunk ports. The value of *vlan-id* is the ID of the VLAN to which secure entries are added. Valid IDs are 1 to 1005; do not enter leading zeroes.

Command Default

Secure addresses are not added to the MAC address table.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2(8)SA	This command was introduced.
11.2(8)SA3	The **vlan** keyword was added.
11.2(8)SA5	The **atm** keyword was added.
12.2(2)XT	This command was implemented on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T, on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command with the **H.H.H** and **maximum** keyword was added for Cisco Series 860 ISRs and Cisco Series 880 ISRs.

Usage Guidelines

Cisco 860 Series ISRs, Cisco 880 Series ISRs, Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

Secure addresses can be assigned to only one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

If the maximum number is more than the MAC addresses statically specified by using the **H.H.H** keyword, the switch learns the MAC address automatically up to the specified maximum. If the maximum number is less than the number of MAC addresses already specified statically, then an error message displays.

Usage Guidelines

Catalyst Switches

Secure addresses can be assigned to only one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

Dynamic-access ports cannot be configured with secure addresses.

Cisco 860 Series ISRs, Cisco 880 Series ISRs

The following example shows how to allow ten devices on Fast Ethernet port 2:

```
Router(config)#
 mac-address-table secure maximum 10 ?
FastEthernet  FastEthernet IEEE 802.3
Router(config)#
 mac-address-table secure maximum 10 f ?
<0-4>  FastEthernet interface number
Router(config)#
mac-address-table secure maximum 10 f 2
```

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

Router(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6

Catalyst Switches

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6
```

The following example shows how to add a secure MAC address to ATM port 2/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa atm 2/1
```

Related Commands

Command	Description
clear mac -address-table	Deletes entries from the MAC address table.
mac -address-tableaging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
mac -address-tabledynamic	Adds dynamic addresses to the MAC address table.

Command	Description
mac -address-tablestatic	Adds static addresses to the MAC address table.
show mac -address-table	Displays the MAC address table.

main-fiber port

To specify the port number to use for the optical link connection on the SDH/STM-1 trunk card on a Cisco AS5850, use the **main-fiberport** command in controller configuration mode.

main-fiber port {**0** | **1**}

Syntax Description

0	Specifies use of port 0 as the optical link connection. This is the default.
1	Specifies use of port 1 as the optical link connection.

Command Default

Port 0

Command Modes

Controller configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the**main-fiber** controller configuration command if you need to use optical port 1 during installation of the SDH/STM-1 trunk card on a Cisco AS5850 or if you suspect some problem with optical port 0.

This command does not have a **no** form. To restore the default value, use the **main-fiberport0**command.

Examples

The following example selects port 1 as the port with the optical connection:

```
Router(config)# controller sonet 1/0
Router(config-controller)# main-fiber port 1
```

max-reserved-bandwidth

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

max-reserved-bandwidth *percent*
no max-reserved-bandwidth

Syntax Description

percent	Percent of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, and Frame Relay PIPQ.

Command Default

75 percent on all supported platforms except the Cisco 7500 series routers, which do not have this restriction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

Examples

In the following example, the policy map called policy1 is configured for three classes with a total of 8 Mbps configured bandwidth, as shown in the output from the **showpolicy-map** command:

```
Router# show policy-map policy1
 Policy Map policy1
  Weighted Fair Queueing
    Class class1
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class2
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class3
      Bandwidth 3000 (kbps) Max Threshold 64 (packets)
```

When you enter the **service-policy**command in an attempt to attach the policy map on a 10-Mbps Ethernet interface, an error message such as the following is produced:

```
I/f Ethernet1/1 class class3 requested bandwidth 3000 (kbps) Available only 2500 (kbps)
```

The error message is produced because the default maximum configurable bandwidth is 75 percent of the available interface bandwidth, which in this example is 7.5 Mbps. To change the maximum configurable bandwidth to 80 percent, use the **max-reserved-bandwidth** command in interface configuration mode, as follows:

```
max-reserved-bandwidth 80
service output policy1
end
```

To verify that the policy map was attached, enter the **showpolicy-mapinterface** command:

```
Router# show policy-map interface e1/1
 Ethernet1/1  output :policy1
  Weighted Fair Queueing
    Class class1
      Output Queue:Conversation 265
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class2
      Output Queue:Conversation 266
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class3
      Output Queue:Conversation 267
        Bandwidth 3000 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
```

Virtual Template Configuration Example

The following example configures a strict priority queue in a virtual template configuration with CBWFQ. The **max-reserved-bandwidth** command changes the maximum bandwidth allocated between CBWFQ and IP RTP Priority from the default (75 percent) to 80 percent.

```
multilink virtual-template 1
interface virtual-template 1
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip rtp priority 16384 16383 25
 service-policy output policy1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 max-reserved-bandwidth 80
 end
interface Serial0/1
 bandwidth 64
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp multilink
 end
```

Note To make the virtual access interface function properly, do not configure the **bandwidth** command on the virtual template. Configure it on the actual interface, as shown in the example.

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
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.
show policy-map	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

mdix auto

To enable automatic media-dependent interface with crossover detection, use the **mdixauto** command in interface configuration mode. To turn automatic detection off, use the **no** form of this command.

mdix auto
no mdix auto

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on all 10/100 and 10/100/1000 modules except for the following modules:

- WS-X6248-RJ45
- WS-X6248-TELCO
- WS-X6348-RJ-45
- WS-X6348-RJ-21
- WS-X6148-RJ-45
- WS-X6148-RJ-21

Examples

This example shows how to enable automatic media-dependent interface with crossover detection:

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

This example shows how to disable automatic media-dependent interface with crossover detection:

```
Router(config-if) no mdix auto
Router(config-if)
```

Related Commands

Command	Description
show interfaces	Displays the status and traffic statistics for the interfaces in the chassis.

mdl

To configure the Maintenance Data Link (MDL) message defined in the ANSI T1.107a-1990 specification, use the **mdl** command in controller configuration mode. To remove the message, use the **no** form of this command.

mdl {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} *string*}
no mdl {**transmit** {**path** | **idle-signal** | **test-signal**} | **string** {**eic** | **lic** | **fic** | **unit** | **pfi** | **port** | **generator**} *string*}

Syntax Description

transmit path	Enables transmission of the MDL Path message.
transmit idle-signal	Enables transmission of the MDL Idle Signal message.
transmit test-signal	Enables transmission of the MDL Test Signal message.
string eic *string*	Specifies the Equipment Identification Code; can be up to 10 characters.
string lic *string*	Specifies the Location Identification Code; can be up to 11 characters.
string fic *string*	Specifies the Frame Identification Code; can be up to 10 characters.
string unit *string*	Specifies the Unit Identification Code; can be up to 6 characters.
string pfi *string*	Specifies the Path Facility Identification Code sent in the MDL Path message; can be up to 38 characters.
string port *string*	Specifies the Port number string sent in the MDL Idle Signal message; can be up to 38 characters.
string generator *string*	Specifies the Generator number string sent in the MDL Test Signal message; can be up to 38 characters.

Command Default

No MDL message is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(13)EX	This command was introduced on the Cisco 7304 router.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2(18)S.

Release	Modification
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPA on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the mdl command to send messages in maintenance data link in T3 c-bit framing mode.



Note MDL is supported only when the DS3 framing is C-bit parity.

Examples

The following example shows the **mdl** commands on a T3 controller in slot 1, port 0:

```
Router(config)# controller t3 1/0
Router(config-controller)# clock source line
Router(config-controller)# mdl string eic ID
Router(config-controller)# mdl string fic Building B
Router(config-controller)# mdl string unit ABC
Router(config-controller)# mdl string pfi Facility Z
Router(config-controller)# mdl string port Port 7
Router(config-controller)# mdl transmit path
Router(config-controller)# mdl transmit idle-signal
```

Related Commands

Command	Description
controller	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controllers serial	Displays serial line statistics.
show controllers t3	Displays information about T3 controllers.

media-type

To specify the physical connection on an interface, use the **media-type** command in interface configuration mode. To restore the default value, use the **no** form of this command.

media-type {**aui** | **10baset** | **100baset** | **mii** | **rj45** | **gbic**}
no media-type {**aui** | **10baset** | **100baset** | **mii**}

Syntax Description

aui	Selects an AUI 15-pin physical connection. This is the default on Cisco 4000 series routers.
10baset	Selects an R-J45 10BASE-T physical connection.
100baset	Specifies an RJ-45 100BASE-T physical connection. This is the default on Cisco 7000 series and Cisco 7200 series routers.
mii	Specifies a media-independent interface.
rj45	Specifies an RJ-45 physical connection. This is the default on Cisco 7304 series routers.
gbic	Specifies a Gigabit Interface Converter (GBIC) or small-form factor pluggable (SFP) physical connection for fiber media.

Command Default

An AUI 15-pin physical connection is the default setting on Cisco 4000 series routers. A 100BASE-T physical connection is the default setting on Cisco 7000 series and Cisco 7200 series routers. An RJ-45 physical connection is the default setting on Cisco 7304 series routers

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1E	Support for Gigabit Ethernet was added with the **gbic** keyword.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S2	This command was implemented on the 2-Port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To specify the physical connection on an interface, use the following interface configuration:

- Ethernet network interface module configuration on Cisco 4000 series routers
- Fast Ethernet Interface Processor (FEIP) on Cisco 7000 series, 7200 series, and 7500 series routers
- Full-duplex or half-duplex mode on a serial interface

Use the **media-type**interface configuration command to modify the default physical media connection type from **rj45** to **gbic** to configure a Gigabit Ethernet interface to support fiber media using a GBIC or SFP optical transceiver.

RJ-45 is the only media type supported by the 4-Port 10/100 Fast Ethernet SPA on the Cisco 7304 router, so the **media-type**command does not apply.

Examples

RJ-45 10BASE-T Example

The following example selects an RJ-45 10BASE-T physical connection on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# media-type 10baset
```

Fast Ethernet on a Cisco 7000 or Cisco 7200 Series Example

The following example specifies a media-independent interface physical connection to Fast Ethernet slot 0, port 1 on the Cisco 7000 or Cisco 7200 series:

```
Router(config)# interface fastethernet 0/1
Router(config-if)# media-type mii
```

Cisco 7500 Series Example

The following example specifies a media-independent interface physical connection to Fast Ethernet slot 0, port adapter 1, port 1 on the Cisco 7500 series:

```
Router(config)# interface fastethernet 0/1/1
Router(config-if)# media-type mii
```

Gigabit Ethernet with SPA on a Cisco 7304 Router Example

The following example configures the second interface (port 1) on a 2-Port 10/100/1000 Gigabit Ethernet SPA for a fiber SFP, where the SPA is installed in the bottom subslot (1) of the MSC, and the MSC is installed in slot 2 of the Cisco 7304 router:

Related Commands

Command	Description
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

media-type auto-failover

To assign primary and secondary failover media on the GE-SFP port enter the **media-typeauto-failover** command in interface configuration mode. To automatically detect which media is connected, use the **no** form of this command.

media-type {**sfp** | **rj45**} **auto-failover**
no media-type

Syntax Description

sfp	Designates the SFP port as the primary media.
rj45	Designates the RJ45 port as the primary media
auto-failover	Configures the port with the primary media for automatic failover from SFP to RJ45 or vice-versa when the system goes down, reloads, and is unable to bring up primary media.

Command Default

No media-type. The primary media is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0 (1) M	This command was introduced.

Examples

The following example shows how to configure the primary media as RJ45 and the secondary failover media as SFP:

```
Router(config-if)# media-type rj45 auto-failover
```

The following example shows how to configure the primary media as SFP and the secondary failover media as RJ45:

```
Router(config-if)# media-type sfp auto-failover
```

The following example shows how to configure the router to automatically detect which media is connected:

```
Router(config-if)# no media-type
```

Related Commands

Command	Description
media-type sfp	Specifies an SFP physical connection.
media-type rj45	Specifies an RJ-45 physical connection.

member subslot

To configure the redundancy role of a line card, use the member subslot command in line card redundancy group mode.

member subslot *slot/subslot* {**primary** | **secondary**}
no member subslot *slot/subslot* {**primary** | **secondary**}

Cisco uBR10012 Universal Broadband Routers

member subslot *slot/subslot* {
protect [**config** *slot/subslot* | **rf-power** [**rf-connector** *rfconnector-value*] {**hccp-delta** *diff-pwr* | **hccp-override** *override-pwr*}] | **working** [**rfsw-slot** *slot-value*] | **revertive** | **reverttime** *value*}

no member subslot *slot/subslot* {
protect [**config** *slot/subslot* | **rf-power** [**rf-connector** *rfconnector-value*] {**hccp-delta** *diff-pwr* | **hccp-override** *override-pwr*}] | **working** [**rfsw-slot** *slot-value*] | **revertive** | **reverttime** *value*}

Syntax Description

slot	Chassis line card slot number.
subslot	Chassis line card subslot number.
primary | secondary	Configures the redundancy role of the line card. • **primary** --Active line card. • **secondary** --Standby line card.
protect	Specifies the protect slot in the line card group.
config *slot/subslot*	(Optional) Specifies the appropriate working interface configuration that is used for the protect interface when a switchover occurs.
rf-power	(Optional) Specifies the RF power output level on an integrated upconverter.
rf-connector *rfconnector-value*	(Optional) Specifies the RF connector in the protect line card. The default value is all.
hccp-delta *diff-pwr*	When using N+1 Hotstandby Connection-to-Connection Protocol (HCCP) redundancy, the protect interface adds the diff-pwr value to the current power value of the working interface when a switchover occurs. This allows the router to accommodate relative differences between the RF power levels in working and protect interfaces. The valid value for diff-pwr ranges from –12 to +12 dBmV.

hccp-override *override-pwr*	When using N+1 HCCP redundancy, the protect interface uses the override power value instead of the power value of the working interface when a switchover occurs. This allows the router to accommodate absolute differences between the RF power levels in working and protect interfaces. The valid value for override-pwr ranges from 45 to 63 dBmV. **Note** The official range for acceptable power levels in the DOCSIS specification is 50 to 61 dBmV. Cisco cable interfaces exceed the DOCSIS standard, but power levels outside the DOCSIS standards should be used only in lab and test environments.
working	Specifies the working slot in the line card group.
rfsw-slot *slot-value*	(Optional) Specifies the RF switch slot for the working line card.
revertive	Specifies the revert operation on the protect card.
reverttime *value*	Specifies the time interval for the revert operation in minutes. If you specify the time interval as 30 minutes, the protect card switches back to the protect mode after 30 minutes.

Command Default

None

Command Modes

Line card redundancy group

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series routers.
12.2(28)BC	This command was integrated into Cisco IOS Release 12.3(23)BC.
12.2(28)SCA	Support for the following keywords was removed in Cisco IOS Release 12.2(33)SCA and later releases: • **revertive** • **reverttime** **Note** Use the revertive command in line card redundancy group mode to enable the revert operation on a protect card in Cisco IOS Release 12.2(33)SCA and later releases.
12.2(28)SCC4	Support for the following keywords was added in Cisco IOS Release 12.2(33)SCC4 for Cisco uBR10012 routers: • **rf-power** • **rf-connector** • **hccp-delta** • **hccp-override**
12.2(28)SCE	The **config** option of the command was made the default. When more than one working line cards are configured, the config option is automatically applied to the first working card.

Usage Guidelines

The primary line card must be the first line card configured and must occupy subslot 1. The secondary line card must be the second line card configured and must occupy subslot 0. Only one primary line card and one secondary line card can be configured.



Note Configuration changes to the working line card cause the upstream links on the protect line card to flap. This is applicable only to Cisco uBR10012 routers.

Examples

The following example creates line card group number 1 for one-to-one line card redundancy. It also specifies the line card in subslot 1 as the primary (active) line card, and the line card in subslot 0 as the secondary (standby) line card:

```
Router(config)# redundancy
Router(config-red)# linecard-group 1 y-cable
Router(config-red-lc)# member subslot 2/1 primary
Router(config-red-lc)# member subslot 2/0 secondary
```



Note The rest of the examples listed here are only applicable to Cisco uBR10012 routers.

The following example shows how to configure a protect interface to add 3 dBmV to the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power hccp-delta 3
```

The following example shows how to configure a protect interface to use an RF power level of 48 dBmV instead of the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power hccp-override 48
```

The following example shows how to configure a rf-connector 3 on a protect interface to add 5 dBmV to the current working RF power level when a switchover occurs:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# linecard-group 1 cable
Router(config-red-lc)# member subslot 5/1 protect rf-power rf-connector 3 hccp-delta 5
```

Related Commands

Command	Description
linecard-group	Creates a line card group for one-to-one line card redundancy.

Command	Description
redundancy	Enters redundancy mode.
show redundancy linecard	Displays information about a redundant line card or line card group.

microcode reload controller

To reload the firmware and field programmable gate array (FPGA) without reloading the Cisco IOS image, use the **microcode reload controller** command in privileged EXEC mode.

microcode reload controller {**t1** | **e1** | **j1**} *x*/*y*

Syntax Description

t1	T1
e1	E1
j1	J1 controller.
x / *y*	Controller slot and unit numbers. The slash must be typed.

Command Default

No microcode reload activity is initiated.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(8)T	The **j1** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Loopbacks in the running configuration are restored after this command is entered. If the controller is in a looped state before this command is issued, the looped condition is dropped. You have to reinitiate the loopbacks from the remote end by entering the **no loop**command from the controller configuration.

Examples

The following example shows how to start the microcode reload activity:

```
Router# microcode reload controller j1 3/0
TDM-connections and network traffic will be briefly disrupted.
Proceed with reload microcode?[confirm]
Router#
*Mar  3 209.165.200.225: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.226: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.227: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state to)
*Mar  3 209.165.200.227: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.228: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: %CONTROLLER-5-UPDOWN: Controller J1 3/0, changed state top
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
*Mar  3 209.165.200.229: clk_src_link_up_down: Status of this CLK does not matter
```

mls exclude protocol

To specify the interface protocol to exclude from shortcutting, use the **mlsexcludeprotocol**command in global configuration mode. To remove a prior entry, use the **no** form of this command.

mls exclude protocol {**both** | **tcp** | **udp**} **port** *port-number*
no mls exclude

Syntax Description

both	Specifies both UDP and TCP.
tcp	Excludes TCP interfaces from shortcutting.
udp	Specifies UDP interfaces from shortcutting.
port *port-number*	Specifies the port number; valid values are from 1 to 65535.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to configure MLS to exclude UDP on port 69:

```
Router(config)#
mls exclude protocol udp port 69
Router(config)#
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.
show mls ipx	Displays MLS IPX information.

mls ip delete-threshold

To delete the configured access control list (ACL) thresholds, use the **mlsipdelete-threshold** comman d in global configuration mode.

mls ip delete-threshold *acl-num*

Syntax Description

acl-num	Reflective ACL number; valid values are from 1 to 10000.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **mlsipdelete-threshold** command is active only when you enable the **mlsipreflexivendr-entrytcam** command.

Examples

This example shows how to delete an ACL threshold:

```
Router(config)# mls ip delete-threshold 223
Router(config)#
```

Related Commands

Command	Description
mls ip install-threshold	Installs the configured ACL thresholds.
mls ip reflexive ndr-entry tcam	Enables the shortcuts in TCAM for the reflexive TCP/UDP entries when installed by the NDR.

mls ip directed-broadcast

To enable the hardware switching of the IP-directed broadcasts, use the **mlsipdirected-broadcast** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mls ip directed-broadcast {**exclude-router** | **include-router**}
no mls ip directed-broadcast

Syntax Description

exclude-router	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN except the router.
include-router	Forwards the IP-directed broadcast packet in the hardware to all hosts in the VLAN including the router.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **exclude-router** and **include-router** keywords both support hardware switching, but **exclude-router** does not send a copy of the hardware-switched packets to the router. If you enter the **include-router** keyword, the router does not forward the IP-directed broadcast packet again.

In the default mode, IP-directed broadcast packets are not hardware forwarded; they are handled at the process level by the MSFC. The MSFC decision to forward or not forward the packet is dependent on the **ipdirected-broadcast** command configuration.

There is no interaction between the **ipdirected-broadcast** command and the **mlsipdirected-broadcast** command. The **ipdirected-broadcast** command involves software forwarding, and the **mlsipdirected-broadcast** command involves hardware forwarding.

MLS IP-directed broadcast supports a secondary interface address.

Any packets that hit the CPU are not forwarded unless you add the **ipdirected-broadcast** command to the same interface.

You can configure the MLS IP-directed broadcasts on a port-channel interface but not on the physical interfaces on the port-channel interface. If you want to add a physical interface to a port-channel group, the physical interface cannot have the MLS IP-directed broadcast configuration. You have to first remove the configuration manually and then add the physical interface to the channel group. If a physical interface is already part of a channel group, the CLI will not accept the **mlsipdirected-broadcast** configuration command on that physical interface.

Examples

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN with the exception of the router:

```
Router(config-if)#
mls ip directed-broadcast exclude-router
Router(config-if)#
```

This example shows how to forward the IP-directed broadcast packet in the hardware to all hosts in the VLAN:

```
Router(config-if)#
mls ip directed-broadcast include-router
Router(config-if)#
```

Related Commands

Command	Description
show mls cef adjacency	Displays information about the MLS-hardware Layer 3-switching adjacency node.

mls ipx

To enable Multilayer Switching (MLS) Internetwork Packet Exchange (IPX) on the interface, use the **mlsipx**command in interface configuration mode. To disable IPX on the interface, use the **no** form of this command.

mls ipx
no mls ipx

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to enable MLS IPX on an interface:

```
Router(config-if)#
mls ipx
Router(config-if)#
```

Related Commands

Command	Description
mls rp ipx (interface configuration mode)	Allows the external systems to enable MLS IPX on the interface.
show mls ipx	Displays MLS IPX information.

mls verify

To enable Layer 3 error checking in the hardware, use the **mlsverify** command in global configuration mode. To disable Layer 3 error checking in the hardware, use the **no** form of this command.

mls verify {**ip** | **ipx**} {**checksum** | **length** {**consistent** | **minimum**}}
no mls verify {**ip** | **ipx**} {**checksum** | **length** {**consistent** | **minimum**}}

Syntax Description

ip	Specifies the IP-checksum errors.
ipx	Specifies the IPX checksum errors.
checksum	Enables the checksum-error check.
length consistent	Enables the length-consistency check in Layer 2.
length minimum	Enables the minimum-length packet check in Layer 2.
consistent	Specifies the length-consistency check in Layer 2.
minimum	Enables the minimum-length packet check in Layer 2.

Command Default

checksum

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was changed to include the **minimum** keyword on the Supervisor Engine 720. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The minimum-length packets are the packets with an IP header length or IP total length field that is smaller than 20 bytes.

When entering the minimum keyword, follow these guidelines:

- When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.



Caution Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible

- When entering the **nomlsverifyiplengthminimum** command, minimum-length packets are hardware switched. The packets that have IP protocol = 6 (TCP) are sent to the software.

Examples

This example shows how to enable Layer 3 error checking in the hardware:

```
Router(config
)# mls verify ip checksum
Router(config)#
```

This example shows how to disable Layer 3 error checking in the hardware:

```
Router(config
)# no mls verify ip checksum
Router(config)#
```

mobility

To configure the wireless mGRE tunnels, use the **mobility** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

mobility {**network-id** *id* | **tcp adjust-mss**}
mobility [**trust** | **broadcast**]

Syntax Description

network-id *id*	Specifies the wireless network ID for the mGRE tunnel; valid values are from 1 to 4095.
tcp adjust-mss	Adjusts the MSS value in TCP SYN and TCP ACK on the access points automatically.
trust	(Optional) Specifies the trusted network.
broadcast	(Optional) Specifies that the mGRE tunnel convert the NBMA to the BMA.

Command Default

Untrusted network

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXD3	This command was changed to include the **tcpadjust-mss** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a WLSM only.

The **tcpadjust-mss** keywords are supported on mGRE tunnel interfaces only.

You can enter the **iptcpadjust-mss***value* command to change the TCP MSS to a lower value.

A trusted network can use DHCP or a static IP address. An untrusted network supports only DHCP clients.

Examples

This example shows how to specify the network identification number for the mGRE tunnel:

```
Router(config-if)# mobility network-id 200
Router(config-if)#
```

This example shows how to specify the trusted network:

```
Router(config-if)# mobility trust
Router(config-if)#
```

This example shows how to specify that the mGRE tunnel convert the NBMA to the BMA:

```
Router(config-if)# mobility broadcast
Router(config-if)#
```

This example shows how to adjust the MSS value in TCP SYN and TCP ACK on the access points automatically:

```
Router(config-if)# mobility tcp adjust-mss
Router(config-if)#
```

Related Commands

Command	Description
ip tcp adjust-mss	Adjusts the MSS value of TCP SYN packets going through a router.
show mobility	Displays information about the Layer 3 mobility and the wireless network.

mode

To set the redundancy mode, use the **mode** command in redundancy configuration mode.

Syntax for 12.2S Release
mode {**rpr** | **rpr-plus** | **sso**}

Syntax for Cisco IOS XE Release 2.5 and Later Releases
mode {**rpr** | **sso**}

Syntax for 12.2XNE Release
mode sso

Syntax Description

rpr	Specifies Route Processor Redundancy (RPR) mode.
rpr-plus	Specifies Route Processor Redundancy Plus (RPR+) mode.
sso	Specifies stateful switchover (SSO) mode.

Command Default

- The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.
- If redundancy is enabled, the default is the mode that you have configured.
- The default is RPR+ mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.
- If redundancy is enabled, the default is the mode that you have configured.
- The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.
- The default is SSO mode if the system is not configured for redundancy and the active and standby supervisor engines have the same image.
- The default is RPR mode if different versions are installed.

Command Modes

Redundancy configuration (config-red)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was modified. Support was added for SSO mode and the default mode change.

Release	Modification
12.2(17d)SXB	This command was modified. Support was added for multicast and unicast traffic.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)XNE	This command was modified. This command was implemented on the Cisco 10000 router.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Cisco IOS Release 12.2S and 7600 Series Routers

SSO is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

On releases prior to Release 12.2(17d)SXB, single router mode (SRM) with SSO redundancy does not support stateful switchover for multicast traffic. When a switchover occurs, all multicast hardware switching entries are removed and are then re-created and reinstalled in the hardware by the newly active multilayer switch feature card (MSFC).

SRM/SSO is supported in the following releases only:

- Release 12.2(17b)SXA and subsequent rebuilds.
- Release 12.2(17d)SXB and subsequent rebuilds.

Nonstop forwarding (NSF) with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

If you have configured MPLS on the Cisco 7600 series routers with redundant supervisor engines, you must configure the Cisco 7600 series router in RPR mode. The switch should not be running in the default mode of SSO.

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

Follow these guidelines when configuring your system for RPR+ mode:

- You must install compatible images on the active and standby supervisor engines to support RPR+ mode and SSO mode.
- Both supervisor engines must run the same Cisco IOS software version.
- Any modules that are not online at the time of a switchover are reset and reloaded on a switchover.
- The Forwarding Information Base (FIB) tables are cleared on a switchover. As a result, routed traffic is interrupted until route tables reconverge.

The standby supervisor engine reloads on any change of mode and begins to work in the current mode. When you use this command to force the standby supervisor engine to run as a Distributed Forwarding Card (DFC) card, the uplink ports in the standby engine continue to be in use and are not disabled.

Cisco IOS Release XE Release 2.5 and ASR 1000 Series Routers

For Cisco ASR 1002 and 1004 routers, RRP and stateful switchover can be used to switch between Cisco IOS processes. RPR and SSO need to be configured by the user, however, because a second Cisco IOS process is not available by default on Cisco ASR 1002 and 1004 routers. Enter the **redundancy** command in global

configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

The Cisco ASR 1006 Router supports a second Route Processor. The second Cisco IOS process can run only on the standby Route Processor. This means that hardware redundancy is available and RPR and SSO do not need to be configured by the user because a second Cisco IOS process is available by default on the Cisco ASR 1006 router.

RPR+ mode is not supported on the Cisco ASR 1000 Series Routers.

Cisco IOS Release 12.2XNE and 1000 Series Routers

Enter the **redundancy** command in global configuration mode to enter redundancy configuration mode. You can enter the **mode** command within redundancy configuration mode.

RPR mode is not supported on the Cisco 10000 router.

Examples

This example shows how to set the redundancy mode to RPR+:

```
Router(config)# redundancy
Router(config-red)# mode rpr-plus
```

This example shows how to set the redundancy mode to SSO:

```
Router(config)# redundancy
Router(config-red)# mode sso
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Forces a switchover from the active to the standby supervisor engine.
route-converge-interval	Configures the time interval after which the old FIB entries are purged.
show redundancy	Displays RF information.
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

mode (ATM T1 E1 controller)

To set the DSL controller into ATM mode and create an ATM interface or to set the T1 or E1 controller into T1 or E1 mode and create a logical T1/E1 controller, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no** form of this command.

Cisco 1800, Cisco 2800, Cisco 3700, Cisco 3800 Series
mode atm
no mode atm

Cisco 1700 Series, Cisco 2600XM
mode {**atm** | **t1** | **e1**}
no mode {**atm** | **t1** | **e1**}

Cisco IAD2430
mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDBC) for E1. When you remove ATM mode by entering the **nomodeatm** command, ATM interface 0 is deleted. **Note** The **modeatm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only; it is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco IAD2430 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis: • Cisco 2600 series--0. • Cisco 3660--0 or 1.
cas	(Cisco 2600 series WIC slots only) Channel-associated signaling (CAS) mode. The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (that is, it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1. On the Cisco IAD2430 series IAD, CAS mode is not supported.

t1	Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

The controller mode is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to the merged SGCP/MGCP software.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for the Cisco IAD2420.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The keyword **aim** and the argument *aim-slot* were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	This command was integrated into Cisco IOS Release 12.3(4)XD on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(4)XG	This command was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T on Cisco 2600 series and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

When a DSL controller is configured in ATM mode, the mode must be configured identically on both the CO and CPE sides. Both sides must be set to ATM mode.

Note If using the **nomodeatm** command to leave ATM mode, the router must be rebooted immediately to clear the mode.

When configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CPE and CO sides.

Examples

ATM Mode Example

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode atm
```

T1 Mode Example

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Configures a list of time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect.

mode (HSA redundancy)

To configure the redundancy mode, use the **mode**command in redundancy configuration mode. To configure the default redundancy mode, use the **no**form of this command.

mode {**hsa** | **rpr** | **rpr-plus**}
no mode {**hsa** | **rpr** | **rpr-plus**}

Syntax Description

hsa	Selects High System Availability (HSA) redundancy mode. This is the default.
rpr	Selects Route Processor Redundancy (RPR) mode.
rpr-plus	Selects Route Processor Redundancy Plus (RPR+) redundancy mode.

Command Default

HSA redundancy mode

Command Modes

Redundancy configuration

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.0(19)ST1	The **rpr-plus**keyword was added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The mode selected by the **mode** command in redundancy configuration mode must be fully supported by the image that has been installed in both the active and standby Route Switch Processors (RSPs). A high availability image must be installed in the RSPs before RPR+ can be configured. Use the**hw-moduleslotimage**command to specify a high availability image to run on the standby RSP.

If the mode cannot be set on both RSPs, HSA is the default mode. A Cisco 7507 or Cisco 7513 router that has only one RSP installed operates in single Route Processor mode.

Examples

The following example enters redundancy configuration mode and sets RPR+ as the redundancy mode for a Cisco 7500 series router.

```
Router(config)# redundancy
Router(config-r)# mode rpr-plus
Router(config-r)# end
```

Related Commands

Command	Description
hw-module sec-cpu reset	Resets and reloads the standby RSP with the specified Cisco IOS image and executes the image.

Command	Description
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RSP.
redundancy	Enters redundancy configuration mode.
redundancy force-switchover	Switches control of a router from the active RSP to the standby RSP.
show redundancy	Displays the current redundancy mode.

mode (RSC redundancy)

To choose between classic-split mode (maximum throughput with no load sharing) and handover-split mode (maximum availability with load sharing), use the **mode** command in redundancy configuration mode. To reset to the default mode, use the **no** form of this command.

mode {**classic-split** | **handover-split**}
no mode

Syntax Description

classic-split	Nonredundant mode in which slots are split in a fixed 6/6 pattern between the two route-switch-controller (RSC) cards, and no handover occurs. This is the default.
handover-split	Redundant mode in which, if one RSC fails, the peer RSC takes over control of the failed RSC's resources (slots and cards).

Command Default

Classic-split mode

Command Modes

Redundancy configuration

Command History

Release	Modification
12.2(2)XB1	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

You must be connected to an RSC card on your Cisco AS5850 to use this command.

Examples

The following example selects handover-split mode:

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

mode handover-split
```

Related Commands

Command	Description
show chassis	Displays, for a router with two RSCs, information about mode (handover-split or classic-split), RSC configuration, and slot ownership.
show chassis clocks	Displays all configured clock sources, even those from non-owned cards. This is because only one RSC can provide the master clock, and it may need to have backup clock sources configured from all cards present, regardless of ownership.
show context	Displays information about specified slots.
show redundancy debug-log	Displays up to 256 redundancy-related debug entries.

mode (T1 E1 controller)

To set the T1 or E1 controller into asynchronous transfer mode (ATM) and create an ATM interface, to set the T1 or E1 controller into T1 or E1 mode and create a logical T1 or E1 controller, or to set the T1 or E1 controller into channel-associated signaling (CAS) mode, use the **mode** command in controller configuration mode. To disable the current mode and prepare to change modes, use the **no**form of this command.

mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}
no mode {**atm** [**aim** *aim-slot*] | **cas** | **t1** | **e1**}

Syntax Description

atm	Sets the controller into ATM mode and creates an ATM interface (ATM 0). When ATM mode is enabled, no channel groups, DS0 groups, PRI groups, or time-division multiplexing (TDM) groups are allowed, because ATM occupies all the DS0s on the T1/E1 trunk. When you set the controller to ATM mode, the controller framing is automatically set to extended super frame (ESF) for T1 or cyclic redundancy check type 4 (CRC4) for E1. The line code is automatically set to binary 8-zero substitution (B8ZS) for T1 or high-density bipolar C (HDB3) for E1. When you remove ATM mode by entering the **no mode atm** command, ATM interface 0 is deleted. On the Cisco MC3810, ATM mode is supported only on controller 0 (T1 or E1 0). **Note** The **mode atm** command without the **aim** keyword uses software to perform ATM segmentation and reassembly (SAR). This is supported on Cisco 2600 series WIC slots only and is not supported on network module slots.
aim	(Optional) The configuration on this controller uses the Advanced Integration Module (AIM) in the specified slot for ATM SAR. The **aim** keyword does not apply to the Cisco MC3810 and the Cisco IAD2420 series IAD.
aim-slot	(Optional) AIM slot number on the router chassis. For the Cisco 2600 series, the AIM slot number is 0; for the Cisco 3660, the AIM slot number is 0 or 1.
cas	(CAS mode on Cisco 2600 series WIC slots only) The T1 or E1 in this WIC slot is mapped to support T1 or E1 voice (it is configured in a DS0 group or a PRI group). CAS mode is supported on both controller 0 and controller 1.
t1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into T1 mode and creates a T1 interface. When you set the controller to T1 mode, the controller framing is automatically set to ESF for T1. The line code is automatically set to B8ZS for T1.
e1	(Cisco 2600XM series using the G.SHDSL WIC only) Sets the controller into E1 mode and creates an E1 interface. When you set the controller to E1 mode, the controller framing is automatically set to CRC4 for E1. The line code is automatically set to HDB3 for E1.

Command Default

No controller mode is configured.

Command Modes

Controller configuration

Command History

Release	Modification
11.3 MA	This command was introduced on the Cisco MC3810.
12.1(5)XM	Support for this command was extended to Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 7200 series.
12.2(2)XB	Support was extended to the Cisco 2600 series and Cisco 3660. The **aim**keyword and the *aim-slot* argument were added. The parenthetical modifier for the command was changed from "Voice over ATM" to "T1/E1 controller."
12.2(8)T	This command was implemented on the Cisco IAD2420 series.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5850.
12.2(15)T	This command was implemented on the Cisco 2691 and the Cisco 3700 series.
12.3(4)XD	Support was extended on Cisco 2600 series and Cisco 3700 series routers to configure DSL Frame mode and to add T1/E1 Framed support.
12.3(7)T	The support that was added in Cisco IOS Release 12.3(4)XD was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

This command has the following platform-specific usage guidelines:

- Cisco 2600 series, Cisco 3660 routers, or Cisco 3700 series that use an AIM for ATM processing must use the **mode atm aim***aim-slot* command.
- Cisco 2600 series routers that use an AIM for DSP processing and specify DS0 groups must use the **mode cas** command if they are using WIC slots for voice. This command does not apply if network modules are being used.
- Cisco 3660 routers or Cisco 3700 series that use an AIM only for DSP resources should not use this command.
- On Cisco 2600 series routers that use WIC slots for voice, the **mode atm** command without the **aim** keyword specifies software ATM segmentation and reassembly. When the **aim** keyword is used with the **mode atm** command, the AIM performs ATM segmentation and reassembly.
- Cisco MC3810 routers cannot use the **aim** keyword.
- Cisco MC3810 routers with digital voice modules (DVMs) use some DS0s exclusively for different signaling modes. The DS0 channels have the following limitations when mixing different applications (such as voice and data) on the same network trunk:
  - On E1 controllers, DS0 16 is used exclusively for either CAS or common channel signaling (CCS), depending on which mode is configured.
  - On T1 controllers, DS0 24 is used exclusively for CCS.

- Cisco MC3810--When no mode is selected, channel groups and clear channels (data mode) can be created using the **channel group** and **tdm-group** commands, respectively.
- Cisco MC3810 is not supported in the AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series, Cisco 3660, and Cisco 3700 Series feature.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in ATM mode, the mode must be set to the same mode on both the CO and CPE sides. Both sides must be set to ATM mode.
  - If the **no mode atm** command is used to leave ATM mode, the router must be rebooted immediately to clear the mode.
- On Cisco 2600 series and Cisco 3700 series routers when configuring a DSL controller in T1 or E1 mode, the mode must be configured identically on the CO and CPE sides.

Examples

The following example configures ATM mode on controller T1 0. This step is required for Voice over ATM.

```
Router(config)# controller
 T1 0
Router(config-controller)# mode atm
```

The following example configures ATM mode on controller T1 1/ 0 on a Cisco 2600 series router using an AIM in slot 0 for ATM segmentation and reassembly:

```
Router(config)# controller
 t1 1/0
Router(config-controller)# mode atm aim 0
```

The following example configures CAS mode on controller T1 1 on a Cisco 2600 series router:

```
Router(config)# controller
 T1 1
Router(config-controller)# mode cas
```

The following example configures ATM mode on the DSL controller.

```
Router(config)# controller
 dsl 3/0
Router(config-controller)# mode atm
```

The following example configures T1 mode on the DSL controller.

```
Router(config)# controller
 dsl
 3/0
Router(config-controller)# mode t1
```

Related Commands

Command	Description
channel-group	Defines the time slots for voice channels on controller T1 0 or E1 0.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

mode bypass

To enable Virtual Multipoint Interfaces (VMI) to support multicast traffic, use the **modebypass** command in interface configuration mode. To return the interface to the default mode of aggregate, use the **no** form of this command.

mode [**aggregate** | **bypass**]
no mode bypass

Syntax Description

aggregate	Sets the mode to aggregate. All virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI.
bypass	Sets the mode to bypass.

Command Default

No mode

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support multicast traffic on Virtual Multipoint Interfaces (VMIs).

Usage Guidelines

Use the mode bypass command when you need to support multicast traffic in router-to-radio configurations.

Aggregate Mode

The default mode for operation of the VMI is **aggregate** mode. In aggregate mode, all of the virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI. As such, applications above Layer 2, such as, EIGRP and OSPFv3, should be defined on the VMI interface only. Packets sent to the VMI will be correctly forwarded to the correct virtual-access interface.

Bypass Mode

Using **bypass** mode is recommended for multicast applications.

In **bypass** mode, the virtual-access interfaces are directly exposed to applications running above Layer2. In bypass mode, definition of a VMI is still required because the VMI will continue to manage presentation of cross-layer signals, such as, neighbor up, neighbor down, and metrics. However, applications will still be aware on the actual underlying virtual-access interfaces and send packets to them directly.

Using **bypass** mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

After you enter the **modebypass** command, Cisco recommends that you copy the running configuration to NVRAM. because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

Examples

The following example sets the interface mode to bypass:

```
Router# enable
Router# configure terminal
Router(config)# interface vmi1
Router(config-if)# mode bypass
```

Related Commands

Command	Description
interface vmi	Creates a VMI interface.

mode c-12

To configure the mode of an E1 line that has been mapped to a TUG-3, use the mode c-12 command in configuration controller tug3 mode.To configure the mode of an E1 line that has been mapped to a AU-3, use the mode c-12 command in configuration controller au3 mode. To disable the mode configuration, use the **no** form of this command.

mode c-12
no mode c-12m

Syntax Description

This command has no arguments or keywords

Command Default

Disabled

Command Modes

Configuration controller tug3 (for an E1 line mapped to a TUG-3) Configuration controller au3 (for an E1 line mapped to an AU-3)

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(7)E	This command was integrated into Cisco IOS Release 12.1(7)E, and support was added for Cisco 7200 VXR routers and Catalyst 6000 family switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can configure each of the TUG-3s or AU-3s of a PA-MC-STM-1 to carry a set of TU-12s (E1s mapped into TU-12s). The **modec-12**command configures the mode of operation of a TUG-3 or AU-3 and specifies that the TUG-3 or AU-3 is divided into 21 TU-12s, each carrying an E1.

Examples

The following example configures the AUG-mapping of the SONET controller to AU-3 and specifies the mode of AU-3 1 to c-12 on a Cisco 7500 series router:

```
Router(config)# controller sonet 1/0/0
Router(config-controller)# aug mapping au-3
Router(config-controller)# au3 1
Router(config-ctrlr-au3)# mode c-12
```

The following example configures the AUG-mapping of the SONET controller to AU-4 and specifies the mode of TUG-3 1 of AU-4 1 to c-12 on a Cisco 7200 VXR router or a Catalyst 6000 family switch:

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

```
Router(config-controller)# aug mapping au-4
Router(config-controller)# au-4 1 tug-3 1
Router(config-ctrlr-tug3)# mode c-12
```

mode ct3

Use this command to configure channelized T3 mode.

mode ct3

Syntax Description

Syntax Description:

There are no keywords for this command.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Examples

The following example shows how to configure DS1 CT3 SAToP mode:

```
Router> enable
Router#configure terminal
Router(config)# controller MediaType 0/5/0
Router(config-ctr)# mode sonet
Router(config-ctr-sonet)# controller sonet 0/5/0
Router(config-ctr-sonet)# rate oc12
Router(config-ctr-sonet)# sts-1 1
Router(config-ctr-sonet)# mode ct3
Router(config-ctr-sonet)# t1 1 cem-group 100 unframed
Router(config-ctr-sonet)# t1 1 framing unframed
Router(config)# interface cem 0/5/0
Router(config-if)#cem 100
Router(config-if)#xconnect 2.2.2.2 10 encapsulation mpls
Router(config-if)#end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.
show controller t3	Displays T3 controller configuration.

mode download

To enable operational code download mode for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **modedownload**command in satellite initial configuration mode. To disable operational code download mode, use the **no** form of this command.

mode download
no mode download

Syntax Description

This command has no arguments or keywords.

Command Default

Operational code download mode is enabled.

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to disable operational code download mode:

```
Router(sat-init-config)# no mode download
```

mode e3

Use this command to configure E3 mode.

mode e3

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

You can change the mode of a controller only when there are no subinterfaces defined for the controller.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
tug-3 1
mode e3
cem-group 100 unframed
end
```

Related Commands

Command	Description
show running configuration	Verifies mode E3 configuration.

mode sonet

Use this command to configure SONET controller configuration mode.

mode sonet

Syntax Description

Syntax Description:

This command has no arguments or keywords.

Command Default

This command is disabled by default; no AIS is sent.

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

This command is used to configure the SONET controller mode.

Examples

The following example shows how to configure SONET mode:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
end
```

Related Commands

Command	Description
controller mediatype	Configures the mediatype controller.
controller sonet	Displays information about Synchronous Optical Network (SONET) controllers.
show controller sonet	Displays SONET controller configuration.

mode sts-nc

To configure the concatenated signals in the SONET network, use the **mode** *sts-nc* command. The concatenated signals are obtained by "gluing" together the payloads of the constituent signals, and they come in fixed sizes. In *SONET*, these are called STS-*N*c Synchronous Payload Envelopes (SPEs), where *N* = 3*X* and *X* is restricted to the values 1, 4, 16, 64, or 256..

mode *sts-nc*

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18 SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

The command is used to concatenate continuous STS into a bundle. supported modes are STS-3c, STS-12c, STS-48c, STS-192c.

Examples

The following example shows the configuration of STS-Nc - contiguous concatenation:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate oc12
sts-1 1-3 mode sts-3c
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

mode t3/e3

To set the T3/E3 controller in T3/E3 mode and create a logical T3/E3 controller, use the mode command in controller configuration mode.

mode t3.e3

Syntax Description

t3/e3	To set the T3/E3controller into T3/E3 mode and create a logical T3/E3 controller, use the mode command in controller configuration mode.

Command Default

The controller mode is disabled.

Command Modes

Controller configuration

Command History

Command History

Release	Modification
XE 3.18SP	This command was introduced.

Usage Guidelines

Use this command to enable the port in T3 mode. When the port is enabled for T3, it can be used for clear channel mode or channelized T3 mode based on configuration.

Examples

The following example shows how to create the local loopback on the controller :

```
Router(config-controller)# mode t3/e3
```

Related Commands

Command	Description
controller media-type	Enters controller configuration mode.

mode two-way

To enable two-way operational mode for the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **modetwo-way**command in satellite initial configuration mode. To revert to one-way operational mode, use the **no** form of this command.

mode two-way
no mode two-way

Syntax Description

This command has no arguments or keywords.

Command Default

Two-way mode is enabled.

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to specify two-way operational mode:

```
Router(sat-init-config)# mode two-way
```

The following example shows how to specify one-way operational mode:

```
Router(sat-init-config)# no mode two-way
```

mode vc-1x

Use this command to configure mode VC-1x mode.

mode vc-1x

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

When you configure mode VC-1x, seven TUG-2 payloads are created. TUG-2 payloads can be of two types, VC-11 and VC-12. Default for TUG-2 payload mode is VC-11. TUG-2 payload VC-11 can be configured as VC or T1 and the range is 1 to 4. TUG-2 payload VC-12 can be configured as VC or E1 and the range is 1 to 3.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm1
no ais-shut
alarm-report all
clock source internal
overhead s1s0 0
aug mapping au-4
au-4 1
clock source internal
mode tug-3
tug-3 1
mode VC1x
tug-2 1 payload VC11
tug-2 2 payload VC11
tug-2 3 payload VC11
tug-2 4 payload VC11
tug-2 5 payload VC11
tug-2 6 payload VC11
tug-2 7 payload VC11
end
```

Related Commands

Command	Description
show running configuration	Verifies mode vc-1z configuration.

mode vc-4

Use this command to configure mode VC4 CEP.

mode vc-4

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

CEP mode is used to encapsulate SDH payload envelopes (SPEs) like VC11, VC12, VC4, or VC4-Nc over PSN. In this mode, the bytes from the corresponding SPE are sent out as they arrive on the TDM line. The interface is considered as a continuous framed bit stream. The packetization of the stream is done according to IETF RFC 4842. The supported ports are STM1, STM4, STM16, and STM64.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm 4
aug mapping au-4
au-4 1
mode vc4
cem-group 100 cep
end
```

Related Commands

Command	Description
show running configuration	Verifies mode VC-4 configuration.

mode vc4-Nc

Use this command to configure mode VC-4 Nc under AU-4.

mode vc4-Nc

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

CEP mode is used to encapsulate SDH payload envelopes (SPEs) like VC11, VC12, VC4, or VC4-Nc over PSN. In this mode, the bytes from the corresponding SPE are sent out as they arrive on the TDM line. The interface is considered as a continuous framed bit stream. The packetization of the stream is done according to IETF RFC 4842. The supported ports are STM1, STM4, STM16, and STM64.

Examples

```
enable
configure terminal
controller sdh 0/5/0
au-4 1-4 mode vc4-4c
cem-group 100 cep
end
```

Related Commands

Command	Description
show running configuration	Verifies configuration.

mode vt-15

To configure the path operation mode, use the **mode vt-15** command in controller configuration STS mode.

mode vt-15

Syntax Description

vt-15	Specifies the mode of operation.

Command Default

None

Command Modes

Controller configuration STS

Command History

Release	Modification
15.1(01)S	This command was introduced on the Cisco 7600 routers.

Examples

This example shows how to configure the **mode vt-15**:

```
Router(config)# controller sonet-acr 1
Router(config-controller)#
sts-1 2
Router(config-ctrlr-sts1)# mode vt-15
```

Related Commands

Command	Description
sts-1	Configures the Synchronous Transport Signal (STS) (level)-1 in the SONET hierarchy.
vtg	Configures the (CESoPSN) CEM group.
controller sonet-acr	Configures the SONET Access Circuit Redundancy (ACR) virtual controller.

mode t3

Use this command to configure T3 mode.

mode t3

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

You can change the mode of a controller only when there are no subinterfaces defined for the controller.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
tug-3 1
mode t3
cem-group 100 unframed
end
```

Related Commands

Command	Description
show running configuration	Verifies configuration.

mode tug-3

Use this command to configure mode Tributary Unit group type 3 (TUG-3) number that has been mapped to an AU-4.

mode tug-3

Syntax Description

Syntax Description

None

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

An AUG of an STM-1 can be derived from either AU-3s or an AU-4. Use the **aug mapping au-4** configuration controller command to map the AUG to a TUG-3. Configuring the **au-4** command enables you to enter configuration controller tug3 command mode and creates a serial interface.

Mode TUG-3 creates three TUG-3 paths. TUG-3 range is 1 to 3.

Examples

```
enable
configure terminal
controller sdh 0/5/0
rate stm4
au-4 1
mode tug-3
end
```

Related Commands

Command	Description
show running configuration	Verifies TUG-3 configuration.

modem dtr-delay

To control the time that a data terminal ready (DTR) signal is held down when a line clears, use the **modemdtr-delay** command in line configuration mode. To restore the default hold down time, use the **no** form of this command.

modem dtr-delay *seconds*
no modem dtr-delay *seconds*

Syntax Description

seconds	Number of seconds. The default is 5.

Command Default

The default DTR signal hold down time is 5 seconds.

Command Modes

Line configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to reduce the time that a DTR signal is held down after an asynchronous line clears and before the DTR signal is raised again to accept new calls. Incoming calls may be rejected in heavily loaded systems even when modems are unused because the default DTR hold down interval may be too long. The**modemdtr-delay** command is designed for lines used for an unframed asynchronous session such as Telnet. Lines used for a framed asynchronous session such as PPP should use the **pulse-time** interface command.

Examples

The following example shows how to specify a DTR hold down interval of 2 seconds:

```
Router(config)# line 7
Router(config-line)# modem dtr-delay 2
```

Related Commands

Command	Description
pulse-time	Enables pulsing DTR signal intervals on serial interfaces.

monitoring

To enable monitoring of all optical transceivers and to specify the time period for monitoring the transceivers, use the **monitoring**command in transceiver type configuration mode. To disable the monitoring, use the **no** form of this command.

monitoring [**interval** *seconds*]
no monitoring [**interval**]

Syntax Description

interval *seconds*	(Optional) Specifies the time interval for monitoring optical transceivers; valid range is 300 to 3600, in seconds, and the default interval time is 600.

Command Default

The interval time is 600 seconds.

Command Modes

Transceiver type configuration (config-xcvr-type)

Command History

Release	Modification
12.2(18)SXE	This command was introduced.
12.2(33)SXH	This command was modified. The**interval** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

You need digital optical monitoring (DOM) feature and transceiver module compatibility information to configure the **monitoring** command. Refer to the compatibility matrix to get the lists of Cisco platforms and minimum required software versions to support Gigabit Ethernet transceiver modules.

Gigabit Ethernet Transceivers transmit and receive Ethernet frames at a rate of a gigabit per second, as defined by the IEEE 802.3-2008 standard. Cisco's Gigabit Ethernet Transceiver modules support Ethernet applications across all Cisco switching and routing platforms. These pluggable transceivers offer a convenient and cost effective solution for the adoption in data center, campus, metropolitan area access and ring networks, and storage area networks.

The **monitoring** command helps you to enable DOM feature and to evaluate threshold violations for all transceiver types. The **interval**keyword enables you to change the default polling interval.For example, if you set the interval as 1500 seconds, this setting causes a delay (of 1500 seconds) for the trap to be sent out by the Simple Network Management Protocol (SNMP) manager running on Cisco IOS software.

Examples

This example shows how to enable monitoring of optical transceivers and set the interval time for monitoring to 1500 seconds:

```
Router# configure terminal
Router(config)# transceiver type all
Router(config-xcvr-type)# monitoring interval 1500
```

This example shows how to disable monitoring for all transceiver types:

```
Router(config-xcvr-type)# no monitoring
```

Related Commands

Command	Description
transceiver type all	Enables monitoring on all transceivers.

mop enabled

To enable an interface to support the Maintenance Operation Protocol (MOP), use the **mopenabled** command in interface configuration mode. To disable MOP on an interface, use the **no** form of this command.

mop enabled
no mop enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on Ethernet interfaces and disabled on all other interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables MOP for serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# mop enabled
```

Related Commands

Command	Description
mop retransmit-timer	Configures the length of time that the Cisco IOS software waits before sending boot requests again to a MOP server.
mop retries	Configures the number of times the Cisco IOS software will send boot requests again to a MOP server.
mop sysid	Enables an interface to send out periodic MOP system identification messages.

mop sysid

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mopsysid** command in interface configuration mode. To disable MOP message support on an interface, use the **no** form of this command.

mop sysid
no mop sysid

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can still run MOP without having the background system ID messages sent. This command lets you use the MOP remote console, but does not generate messages used by the configurator.

Examples

The following example enables serial interface 0 to send MOP system identification messages:

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

Related Commands

Command	Description
mop device-code	Identifies the type of device sending MOP sysid messages and request program messages.
mop enabled	Enables an interface to support the MOP.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes* **mtu command**
no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The table below lists default MTU values according to media type.

Table 1: Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if) Connect configuration (xconnect-conn-config) xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	This command was modified. This command was updated to support the connect configuration mode for Frame Relay Layer 2 interworking.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command supports the xconnect subinterface configuration mode.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies but cannot be set to a value less than 64 bytes.

Note The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Changing the MTU size on a Cisco 7500 series router results in the recarving of buffers and resetting of all interfaces. The following message is displayed: RSP-3-Restart:cbus complex .

You can configure native Gigabit Ethernet ports on the Cisco 7200 series router to a maximum MTU size of 9216 bytes. The MTU values range from 1500 to 9216 bytes. The MTU values can be configured to any range that is supported by the corresponding main interface.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ipmtu** command, for example). If the value specified with the **ipmtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ipmtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ipmtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, the MTU on a subinterface is equal to the default MTU (4490 bytes). A client is configured with the range supported by the corresponding main interface. The MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

VRF-Aware Service Infrastructure Interfaces

The mtu command does not support the VRF-Aware Service Infrastructure (VASI) type interface.

Cisco 7600 Valid MTU Values

On the Cisco 7600 platform, the following valid values are applicable:

- For the SVI ports: from 64 to 9216 bytes
- For the GE-WAN+ ports: from 1500 to 9170 bytes
- For all other ports: from 1500 to 9216 bytes

You can receive jumbo frames on access subinterfaces also. The MTU values can be configured to any range that is supported by the corresponding main interface. If you enable the jumbo frames, the default is 64 bytes for the SVI ports and 9216 bytes for all other ports. The jumbo frames are disabled by default.

Cisco uBR10012 Universal Broadband Router

While configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco uBR10012 router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following overhead:
  - Layer 2 header--14 bytes
  - Dot1Q header--4 bytes
  - CRC--4 bytes
- If you are using MPLS, be sure that the **mplsmtu** command is configured with a value less than or equal to the interface MTU.
- If you are using MPLS labels, you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.



Note For the Gigabit Ethernet SPAs on the Cisco uBR10012 router, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the maximum configurable MTU is 9000 bytes.

Examples

The following example shows how to specify an MTU of 1000 bytes:

```
Router(config)# interface serial 1
Router(config-if)# mtu 1000
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to specify an MTU size on a Gigabit Ethernet SPA on the Cisco uBR10012 router:

```
Router(config)# interface GigabitEthernet3/0/0
Router(config-if)# mtu 1800
```

Related Commands

Command	Description
encapsulation smds	Enables SMDS service on the desired interface.
ip mtu	Sets the MTU size of IP packets sent on an interface.

national bit (controller)

To set the E3 national bit in the G.751 frame used by the E3 controller, use the national bit command in controller configuration mode. To return to the default E3 controller national bit, use the no form of this command.

national bit {**0** | **1**}
no national bit

Syntax Description

0	Sets the E3 national bit in the G.751 frame to 0.
1	Sets the E3 national bit in the G.751 frame to 1. This is the default.

Command Default

The default value is 1.

Command Modes

Controller configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

When G.751 framing is used, bit 11 of the G.751 frame is reserved for national use and is set to 1 by default.

Configure national bit 1 only when required for interoperability with your telephone company.

To verify the national bit configured on the interface, use the **showcontrollersserial** EXEC command.

Examples

The following example sets the national bit to 1 on an E3 controller in slot 1, port 0:

```
Router(config)# controller e3 1/0
Router(config-controller)# national bit 1
```

Related Commands

show controllers serial	Displays information that is specific to the interface hardware.

national bit (interface)

To set the E3 national bit in the G.751 frame used by the PA-E3 port adapter, use the **nationalbit**command in interface configuration mode. To return to the default E3 interface national bit, use the **no** form of this command.

national bit {**0** | **1**}
no national bit

Syntax Description

0	Sets the E3 national bit in the G.751 frame to 0. This is the default.
1	Sets the E3 national bit in the G.751 frame to 1.

Command Default

The default value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	This command was introduced.

Usage Guidelines

The **nationalbit** command sets bit 12 in the E3 frame.

To verify the national bit configured on the interface, use the **showcontrollersserial** EXEC command.

Examples

The following example sets the national bit to 1 on the PA-E3 port adapter in slot 1, port adapter slot 0, interface 0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# national bit 1
```

Related Commands

Command	Description
international bit	Sets the E3 international bit in the G.751 frame used by the PA-E3 port adapter.
show controllers serial	Displays information that is specific to the interface hardware.

national reserve

To set the E1 national bit, use the**nationalreserve**command in interface configuration mode. To return to the default E1 national bit, use the**no** form of this command.

national reserve {**0** | **1**} {**0** | **1**} {**0** | **1**} {**0** | **1**} {**0** | **1**} {**0** | **1**}
no national reserve

Syntax Description

0	Sets any of the six required E1 national bits in the G.751 frame to 0.
1	Sets any of the six required E1 national bits in the G.751 frame to 1. This is the default.

Command Default

111111

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)XE1	This command was implemented on the Cisco 7100 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only for E1. This command not only sets the national reserve bits but also sets the international bit as well. The far left digit represents the international bit. All six digits must be present for the pattern to be valid.

Examples

On Cisco 7100 series routers, the following example sets the E1 national bit on interface 1 on the port adapter in slot 0 to no scrambling:

```
Router(config)# interface atm 1/0
Router(config-if)# national reserve 011011
```

negotiation

To enable advertisement of speed, duplex mode, and flow control on a Gigabit Ethernet interface, use the**negotiation**command in interface configuration mode. To disable automatic negotiation, use the **nonegotiationauto** command.

negotiation {**forced** | **auto**}
no negotiation auto

Syntax Description

forced	Disables flow control and configures the Gigabit Ethernet interface in 1000/full-duplex mode. This keyword is not supported on the 2-port 10/100/1000 Gigabit Ethernet shared port adapter (SPA) on the Cisco 7304 router.
auto	Enables the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface. This is the default.

Command Default

Autonegotiation is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(7)S	This command was modified. The forced keyword was added.
12.0(6)T	This command was modified. The forced keyword was added.
12.1(3a)E	This command was integrated into Cisco IOS Release 12.1E and implemented on the Cisco 7200-I/O-GE+E controller.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(20)S2	This command was implemented on the 2-port 10/100/1000 Gigabit Ethernet SPA on the Cisco 7304 router. The **forced** keyword is not supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

The **negotiation**command is applicable to the Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E and interfaces on the 2-port 10/100/1000 Gigabit Ethernet SPA that are using fiber media. The **negotiationauto**command is used instead of the **duplex** and **speed** commands (which are used on Ethernet and Fast Ethernet interfaces, and interfaces on the 2-port 10/100/1000 Gigabit Ethernet SPA that are using RJ-45 media) to automatically configure the duplex and speed settings of the interfaces.

The **negotiationforced** command is used to configure the Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E to be 1000/full-duplex only and to disable flow control. The **negotiationforced** command is not supported by the 2-port 10/100/1000 Gigabit Ethernet SPA.

The Gigabit Ethernet interface of the Cisco 7200-I/O-GE+E and the interfaces on the 2-port 10/100/1000 Gigabit Ethernet SPA that are using fiber media are restricted to 1000 Mbps/full-duplex only. Autonegotiation advertises and negotiates only to these values.

The **nonegotiationauto** command is used to disable the autonegotiation in the Cisco 3800 series routers. If the speed is set to 1000 Mbps and full-duplex is set for the Gigabit Ethernet interface in small form-factor pluggable (SFP) mode, then the autonegotiation is disabled (forced mode) using the **nonegotiationauto** command.

However, for RJ-45 media the autonegotiation is always enabled for fixed speed and duplex setting. For SFP mode of operation, the autonegotiation can be disabled by using the **nonegotiationauto** command.

Cisco uBR10012 Universal Broadband Router

Autonegotiation is enabled by default and can be disabled on the 5-port Gigabit Ethernet SPA. During autonegotiation, advertisement for flow control, speed, and duplex occurs. If autonegotiation is disabled on one end of a link, it must be disabled on the other end of the link. If one end of a link has autonegotiation disabled and the other end of the link does not, the link does not come up properly on both ends. Flow control is always negotiated when autonegotiation is enabled.

Note Autonegotiation is not supported on the 1-port 10-Gigabit Ethernet SPA in Cisco IOS Release 12.2(33)SCB.

Examples

The following example shows how to enable the second interface (port 1) on a 2-port 10/100/1000 Gigabit Ethernet SPA for autonegotiation, where the SPA is installed in the bottom subslot (1) of the modular services card (MSC), and the MSC is installed in slot 2 of the Cisco 7304 router:

```
Router(config)# interface gigabitethernet 2/1/1
Router(config-if)# media-type gbic
Router(config-if)# negotiation auto
```

The following example shows how to disable the second interface (port 1) on a 2-port 10/100/1000 Gigabit Ethernet SPA for autonegotiation, where the SPA is installed in the bottom subslot (1) of the MSC, and the MSC is installed in slot 2 of the Cisco 7304 router:

```
Router(config)# interface gigabitethernet 2/1/1
Router(config-if)# no negotiation auto
```

Related Commands

Command	Description
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

neighbor (VPLS)

To specify the type of tunnel signaling and encapsulation mechanism for each Virtual Private LAN Service (VPLS) peer, use the **neighbor** command in L2 VFI manual configuration mode. To disable a split horizon, use the **no** form of this command.

neighbor *remote-router-id vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*} [**no-split-horizon**]
no neighbor *remote-router-id* [*vc-id*]

Syntax Description

remote-router-id	Remote peer router identifier. The remote router ID can be any IP address, as long as it is reachable.
vc-id	32-bit identifier of the virtual circuit between the routers.
encapsulation	Specifies tunnel encapsulation.
encapsulation-type	Specifies the tunnel encapsulation type; valid values are **l2tpv3** and **mpls**.
pw-class	Specifies the pseudowire class configuration from which the data encapsulation type is taken.
pw-name	Name of the pseudowire class.
no-split-horizon	(Optional) Disables the Layer 2 split horizon forwarding in the data path.

Command Default

Split horizon is enabled.

Command Modes

L2 VFI manual configuration (config-vfi)

Command History

Release	Modification
12.2(18)SXF	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. This command was updated so that the remote router ID need not be the LDP router ID of the peer.
Cisco IOS XE Release XE 3.7S	This command was integrated into Cisco IOS XE Release XE 3.7S.

Usage Guidelines

In a full-mesh VPLS network, keep split horizon enabled to avoid looping.

With the introduction of VPLS Autodiscovery, the remote router ID no longer needs to be the LDP router ID. The address that you specify can be any IP address on the peer, as long as it is reachable. When VPLS Autodiscovery discovers peer routers for the VPLS, the peer router addresses might be any routable address.

Examples

This example shows how to specify the tunnel encapsulation type:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls
```

This example shows how to disable the Layer 2 split horizon in the data path:

```
Device(config-vfi)# l2 vfi vfi-1 manual
Device(config-vfi)# vpn 1
Device(config-vfi)# neighbor 172.16.10.2 4 encapsulation mpls no-split-horizon
```

Related Commands

Command	Description
l2 vfi manual	Creates a Layer 2 VFI.

network-clock (BITS)

To configure BITS port signaling types, use the **network-clock**command in global configuration mode. To disable the BITS port signaling types, use the **no** form of this command.

network-clock slot *slot* **bits** *number* {**2m** | **e1** [**crc4**] | **j1** [**esf**] | **t1** [**d4** | **esf** [**133ft** | **266ft** | **399ft** | **533ft** | **655ft**]]}
no network-clock slot *slot* **bits** *number* {**2m** | **e1** [**crc4**] | **j1** [**esf**] | **t1** [**d4** | **esf** [**133ft** | **266ft** | **399ft** | **533ft** | **655ft**]]}

Syntax Description

slot	Selects the slot.
slot	Specifies backplane slot number.
bits	Specifies BITS port signaling types.
number	Specifies the BITS port number starting from 0.
2m	Specifies 2.048 MHz square wave signal type.
e1	Specifies E1 signal type.
j1	Specifies Japan J1 signal type.
t1	Specifies T1 signal type.
crc4	E1 CRC4 framing mode.
esf	T1 ESF framing mode.
d4	T1 D4 framing mode.
133ft	Line Build-Out Select 0 to 133 feet.
266ft	Line Build-Out Select 0 to 266 feet.
399ft	Line Build-Out Select 0 to 399 feet.
533ft	Line Build-Out Select 0 to 533 feet.
655ft	Line Build-Out Select 0 to 655 feet.

Command Default

T1, ESF, 133ft

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco series 7600 router for the 76-ES+XT-2TG3CXL and 76-ES+XT-4TG3CXL.

Usage Guidelines

For 76-ES+XT-2TG3CXL and 76-ES+XT-4TG3CXL line cards, the BITS port number is always 0 because there is only one BITS port.

Examples

The following example shows how to configure the BITS port and 10GE interface as clock sources:

```
Router(config)# network-clock select 2 slot 1 ?
  bits    Network clock source is bits interface
  global  Configure the source as global
  local   Configure the source as local
  <cr>

Router(config)# network-clock select 2 slot 1 bits 0 ?
  global  Configure the source as global
  local   Configure the source as local
  <cr>

Router(config)# network-clock select 3 ?
  controller  Select the controller that should source the clock
  interface   Select the interface that should source the clock
  slot        Select the slot that should source the clock
  system      Select the system clock as source

Router(config)# network-clock select 3 interface TenGigabitEthernet 1/1
```

The following example shows how to configure the BITS port signal type and framing mode:

```
Router(config)# network-clock slot 1 bits 0 ?
  2m  2.048MHz square wave signal type
  e1  E1 signal type
  j1  Japan J1 signal type
  t1  T1 signal type

Router(config)# network-clock slot 1 bits 0 t1 ?
  d4   T1 D4 framing mode
  esf  T1 ESF framing mode

Router(config)# network-clock slot 1 bits 0 t1 d4 ?
  133ft  Line Build-Out Select 0 to 133 feet
  266ft  Line Build-Out Select 133 to 266 feet
  399ft  Line Build-Out Select 266 to 399 feet
  533ft  Line Build-Out Select 399 to 533 feet
  655ft  Line Build-Out Select 533 to 655 feet

Router(config)# network-clock slot 1 bits 0 j1 ?
  esf  J1 ESF framing mode

Router(config)# network-clock slot 1 bits 0 e1 ?
  crc4  E1 CRC4 framing mode

Router(config)# network-clock slot 1 bits 0 2m ?
  <cr>
```

Related Commands

Command	Description
show network-clocks	Displays the current configured and active network clock sources.

Command	Description
show platform hardware network-clocks	Displays network clocks for an ES+ line card.

network-clock clear lockout

To clear the lock-out on a clock source, use the network-clock clear lockout command in the privileged EXEC mode.

Cisco 7600 Series Routers
network-clock clear lockout interface *slot/card/port* | **external** *slot/card/port* **2048K** | **e1** {**cas** | **crc4** | **fas**}

Cisco ASR 1000 Series Routers
network-clock clear lockout external {*slot/card/port* | **R0** | **R1**} **T1** {**d4** | **esf** | **sf**}

Syntax Description

external	Specifies external interface (BITS/SSU/GPS).
slot/card/port	Slot number/Card number/Port number.
R0	Specifies the network synchronization mcprp RP0 bits for source slot.
R1	Specifies the network synchronization mcprp RP1 bits for source slot.
T1	Specifies the T1 signal mode input.
d4	Specifies the D4 super frame signal mode.
esf	Specifies the extended super frame signal mode.
sf	Specifies the super frame signal mode.
2048k	Specifies the option 1 2048KHz on the BITS/SSU port.
e1	Specifies the E1 signal mode.
cas	Specifies the E1 Channel Associated Signal (CAS) mode.
crc4	Specifies the E1 with crc4 signal mode.
fas	Specifies the E1 Frame Alignment Signal mode.

Command Default

No default values are available.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.

Examples

The following example shows how to clear the lock out on a clock source:

```
C7600(config)# network-clock clear lockout external 0/0/0 e1 2048k
ASR1000(config)# network-clock clear lockout external 0/0/0 t1 esf
```

network-clock hold-off global

To configure the hold-off time, use the network-clock hold-off global command in the global configuration mode.

network-clock hold-off *timer* **global**

Syntax Description

timer	Hold-off time, in milliseconds. The range is from 50 to 10000. The default is 300. If you do not want the hold off time, set the timer value to 0.
global	Configures the hold-off timer globally.

Command Default

The default value is 300 milliseconds on Cisco ASR 901 Series Aggregation Services Routers.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The hold-off timer can also be configured in the interface configuration mode. It displays a warning message for values below 300 milliseconds and above 1800 milliseconds.

Examples

The following example shows how to configure the hold-off timer in the global configuration mode:

```
Router(config)# network-clock hold-off 50 global
```

network-clock input-source

To assign a controller to be the primary or secondary clock source use the **network-clock input-source***priority* command. To set the controller to be a primary clock source, set the value of priority for the input source to be low value, such as 2, (a low value indicates a high priority). To remove the clock source, use the **no** form of this command

network-clock input-source *priority* **controller t1/e1***slot/bay/port*

no network-clock input-source *priority* **controller t1/e1** *slot/bay/port*

Syntax Description

network-clock input-source *priority*	The network-clock input-source priority command selects the configured controller clock as the backplane clock source.
controller t1/e1	Sets the controller into T1 or E1 signal mode.
priority	Sets the controller to be a primary clock source.
slot/bay/port	Specifies slot, bay and port number

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.
XE Everest 16.5.1	This command was introduced on the Cisco ASR 900 Series Routers and Cisco NCS 4200 Series.

Usage Guidelines

This command is used to assign controller to be the primary or secondary clock source.

Examples

```
enable
configure terminal
network-clock input-source 1controller E1/T10/5/0
```

network-clock set lockout

To lock out a clock source, use the network-clock set lockout command in the privileged EXEC mode. On the Cisco ASR 901 Series Aggregation Services Routers, use the **network-clock clear lockout** command to remove the lockout in global configuration mode.

Cisco 7600 Series Routers
{**network-clock set lockout internal** *slot/card/port* | **external** *slot/card/port* **2048K** | **e1** {**cas** | **crc4** | **fas**}}

Cisco ASR 1000 Series Routers
network-clock set lockout external {*slot/card/port* | **R0** | **R1**} **T1** {**d4** | **esf** | **sf**}

Cisco ASR 901 Cisco ASR 901 Series Aggregation Services Routers
network-clock set lockout {**interface** *interface-name slot/port* | **external** *slot/card/port*}
network-clock clear lockout

Syntax Description

external	Specifies external interface (BITS/SSU/GPS).
slot/card/port	Slot number/card number/port number.
R0	Specifies the network synchronization mcprp RP0 bits for the source slot.
R1	Specifies the network synchronization mcprp RP1 bits for the source slot.
T1	Specifies the T1 signal mode input.
d4	Specifies the D4 super frame signal mode.
esf	Specifies the extended super frame signal mode.
sf	Specifies the super frame signal mode.
2048k	Specifies the option 1 2048KHz on the BITS/SSU port.
e1	Specifies the E1 signal mode.
cas	Specifies the E1 Channel Associated Signal (CAS) mode.
crc4	Specifies the E1 with crc4 signal mode.
fas	Specifies the E1 Frame Alignment Signal mode.
interface	Specifies the interface.
interface-name	Specifies the interface name.

Command Default

No default values are available.

Command Modes

- Global configuration (config)
- Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers. The *interface-name* argument was added.

Usage Guidelines

The **network-clock set lockout** command locks out a clock source. A locked out clock source is not selected for SyncE.

To clear the lock-out on a source, use the **network-clock clear lockout** command.



Note Lock-out takes precedence over force switch, and force switch overrides the manual switch.

Examples

The following example shows how to lock out a clock source:

```
C7600(config)# network-clock set lockout external 2/0/0 e1 cas
ASR1000(config)# network-clock set lockout external R0 t1 esf
```

This example shows how to lockout the clock source on a Cisco ASR 901 Series Aggregation Services Router.

```
Router(config)# network-clock set lockout interface GigabitEthernet 0/1
```

network-clock synchronization ssm option

To configure the equipment to work in a synchronization network, use the **network-clock synchronization ssm option** command in the global configuration mode. To unconfigure the network-clock synchronization option, use the no form of this command.

network-clock synchronization ssm option option_id {**1** | **2** {**GEN1** | **GEN2**}}
no network-clock synchronization ssm option option_id {**1** | **2** {**GEN1** | **GEN2**}}

Syntax Description

option_id	The option_id can have the following values: • 1 - Refers to the synchronization networks design for Europe. This is the default value. (E1 framings are compatible with this option). • 2 - Refers to the synchronization networks design for the U.S. (T1 framings are compatible with this option).
GEN1	If option 2 is configured, then it specifies the generation ID as 1.
GEN2	If option 2 is configured, then it specifies the generation ID as 2.

Command Default

No default values are available.

Cisco ASR 901 Series Aggregation Services Routers

Option 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Network-clock configurations that are not common between options need to be configured again.

On Cisco ASR 901 Series Aggregation Services Routers, the default value for the option_id keyword is 1. If you set the value to 2, you must specify the generation ID.

Examples

The following example shows how the **network-clocksynchronizationssmoption** command is used to configure the equipment to work in a synchronization network:

```
Router> enable
Router# configure terminal
Router(config)# network-clock synchronization automatic
Router(config)# network-clock synchronization ssm option 2 GEN1
```

Related Commands

Command	Description
network-clock eec	Configures the clocking system hardware with the desired parameters.

network-clock synchronization automatic

To enable the network clock synchronization selection process, use the network-clock synchronization automatic command in the global configuration mode. To disable the network clock synchronization selection process, use the no form of this command.

network-clock synchronization automatic
no network-clock synchronization automatic

Syntax Description

This command has no arguments or keywords.

Command Default

No default values are available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.

Usage Guidelines

This command disables the Cisco-specific network-clock process, and turns on G.781-based automatic clock synchronization selection process.

Examples

The following example shows how the network-clock synchronization automatic command is used to enable the network clock synchronization selection process:

```
Router(config)# network-clock synchronization automatic
```

network-clock synchronization mode QL-enabled

To configure the automatic selection process for the QL-enabled mode, use the network-clock synchronization mode QL-enabled command in the global configuration mode.

network-clock synchronization mode QL-enabled

Syntax Description

This command has no arguments or keywords.

Command Default

No default values are available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.
15.1(2)SNH	This command was introduced in Cisco ASR 901 Aggregation Services Routers.

Usage Guidelines

The automatic selection process for the QL-enabled mode is successful only if the Synchronous Ethernet interfaces are capable of sending Synchronization Status Messages (SSM).

Examples

The following example shows how to configure network clock synchronization (QL-enabled mode) in the global configuration mode:

```
Router(config)# network-clock synchronization mode QL-enabled
```

network-clock quality-level

To configure the Quality Level (QL) value for the Synchronization Status Messages (SSM) on a BITS port, use the network-clock quality-level command in the global configuration mode.

Cisco 7600 Series Routers
{**network-clock quality-level** {**rx** | **tx**} {**QL-PRC** | **QL-SSU-A** | **QL-SSU-B** | **QL-SEC** | **QL-DNU**} **external** *slot/card/port* **2048K** | **e1** {**cas** | **crc4** | **fas**}}

Cisco ASR 1000 Series Routers
network-clock quality-level {**rx** | **tx**} {**QL-PRS** | **QL-STU** | **QL-ST2** | **QL-TNC** | **QL-ST3** | **QL-ST3E** | **QL-SMC** | **QL-ST4** | **QL-DUS**} **external** {*slot/card/port* | **R0** | **R1**} **T1** {**d4** | **esf** | **sf**}

Syntax Description

rx	Specifies the received QL. The following values are available on Cisco ASR 1000 Series routers for the QL receive: • QL-PRS • QL-STU • QL-ST2 • QL-ST3 • QL-SMC • QL-ST4 • QL-DUS The following values are available on Cisco 7600 Series routers for the QL receive: • QL-PRC • QL-SSU-A • QL-SSU-B • QL-SEC • QL-DNU

tx	Specifies the trasmitted QL. The following values are available on Cisco ASR 1000 Series routers for the QL transmit: • QL-PRS • QL-STU • QL-ST2 • QL-ST3 • QL-SMC • QL-ST4 • QL-DUS The following values are available on Cisco 7600 Series routers for the QL transmit: • QL-PRC • QL-SSU-A • QL-SSU-B • QL-SEC • QL-DNU
external	Specifies the external interface (BITS/SSU/GPS).
slot /*card*/*port*	Slot number/Card number/Port number.
R0	Specifies the network synchronization RP0 bits for source slot.
R1	Specifies the network synchronization RP1 bits for source slot.
T1	Specifies the T1 signal mode output.
d4	Specifies the D4 super frame signal mode.
esf	Specifies the extended super frame signal mode.
sf	Specifies the super frame signal mode.
2048k	Specifies the option 1 2048KHz on the BITS/SSU port.
e1	Specifies the E1 signal mode.
cas	Specifies the E1 Channel Associated Signal (CAS) mode.
crc4	Specifies the E1 with crc4 signal mode.
fas	Specifies the E1 Frame Alignment Signal mode.

Command Default No default values are available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2.0S	This command was integrated into Cisco ASR 1000 Series routers.
Cisco IOS Release 12.2(33)SRE	This command was introduced on the Cisco 7600 Series routers.

Examples

The following example shows how to configure network-clock quality-level command in the global configuration mode:

```
C7600(config)# network-clock quality-level rx ql-prc external 0/0/0 e1 cas
ASR1000(config)# network-clock quality-level tx QL-ST2 external R0 t1 sf
```

no channelized

To configure the T3 controller for unchannelized mode, use the**nochannelized**configuration controller command. To configure channelized mode, use the **channelized**form of this command.

channelized
no channelized

Syntax Description

This command has no arguments or keywords.

Command Default

MTU size is set to 4470.

Command Modes

Configuration controller

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.1(5a)E	This command was integrated into Cisco IOS Release 12.1(5a)E.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the no channelized configuration controller command to configure the T3 controller for unchannelized mode. When you configure the PA-MC-2T3+ on a Cisco 7500 series router with the no channelized command, the MTU size is set to 4470. In channelized mode, the default MTU size is 1500. The change in MTU sizes will cause a memory recarve and CBus complex to occur, disrupting all traffic on the router for several minutes.

The following message will be displayed when switching between channelized and unchannelized modes on a Cisco 7500 series router:

```
Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]:
Y
```

Type Y for “yes” at the end of the warning. At the prompt, type ^Z to exit. You will exit configuration mode and enter unchannelized mode.

Examples

The following example configures unchannelized mode on a PA-MC-2T3+ in port adapter slot 1 of a VIP2 or VIP4 in a Cisco 7500 series router:

```
configure terminal
  controller T3 1/1/0
  no channelized
```

```
Change to subrate mode will cause cbus complex reset. Proceed? [yes/no]: Y
  ^Z
```

nrzi-encoding

To enable nonreturn-to-zero inverted (NRZI) line-coding format, use the **nrzi-encoding**command in interface configuration mode. To disable this capability, use the **no** form of this command.

nrzi-encoding [**mark**]
no nrzi-encoding

Syntax Description

mark	(Optional) Specifies that NRZI mark encoding is required on the PA-8T and PA-4T+ synchronous serial port adapters on Cisco 7200 and Cisco 7500 series routers . If the **mark** keyword is not specified, NRZI space encoding is used.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **mark** keyword was added for the Cisco 7200 series routers and Cisco 7500 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All FSIP, PA-8T, and PA-4T+ interface types support nonreturn-to-zero (NRZ) and NRZI format. This is a line-coding format that is required for serial connections in some environments. NRZ encoding is most common. NRZI encoding is used primarily with EIA/TIA-232 connections in IBM environments.

Examples

The following example configures serial interface 1 for NRZI encoding:

```
Router(config)# interface serial 1
Router(config-if)# nrzi-encoding
```

The following example configures serial interface 3/1/0 for NRZI mark encoding:

```
Router(config)# interface serial 3/1/0
Router(config-if)# nrzi-encoding mark
```