

A through B

- 1pps, on page 3
- ais-core-failure, on page 4
- ais-shut, on page 5
- alarm-interface, on page 6
- alarm-profile, on page 7
- alarm-profile attach, on page 9
- alarm report all, on page 11
- als, on page 13
- als restart, on page 14
- als restart mode, on page 15
- als restart pulse, on page 16
- analysis-module monitoring, on page 18
- announce interval, on page 20
- announce timeout, on page 21
- anti-jam, on page 22
- apply (satellite initial configuration), on page 23
- aps authenticate, on page 25
- aps adm, on page 26
- aps clear sonet, on page 27
- aps force, on page 28
- aps force sonet, on page 30
- aps group, on page 32
- aps hspw-icrm-grp, on page 34
- aps lockout, on page 37
- aps lockout sonet, on page 38
- aps manual, on page 39
- aps manual sonet, on page 41
- aps protect, on page 43
- aps protect (SONET), on page 44
- aps revert, on page 45
- aps timers, on page 46
- aps unidirectional, on page 47
- aps working, on page 49

- associate slot, on page 51
- association, on page 54
- attach profile-name, on page 55
- atm sonet, on page 57
- au-3, on page 58
- au-4 tug-3, on page 59
- aug mapping, on page 60
- aug mapping [au-3 | au-4] stm [stm number] stm1 number [number], on page 62
- aug mapping au-3 stm [stm number] path number [path number], on page 63
- auto-polarity, on page 64
- b2 sd-ber, on page 65
- b2 sf-ber, on page 66
- backup delay, on page 67
- backup interface, on page 68
- backup interface atm, on page 70
- backup interface cem, on page 72
- backup load, on page 74
- bandwidth (interface configuration), on page 75
- batch, on page 78
- bert abort controller, on page 80
- bert controller, on page 82
- bert errors, on page 86
- bert pattern, on page 87
- bert pattern (T1 E1), on page 89
- bert pattern (T3 E3), on page 91
- bert profile, on page 93
- bitswap line, on page 95
- bridge-domain, on page 96
- bridge-domain (subinterface), on page 101

1pps

To configure the pulse per second parameters of the global navigation satellite system (GNSS) module on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers, use the **1pps** command in the gnss mode. To remove the 1pps configuration, use the **no** form of this command.

1pps {**offset** | **polarity [negative]**}
no 1pps {**offset** | **polarity negative**}

Syntax Description

offset	Configures the 1PPS cable compensation. The valid values are from 0 to 1000 nano seconds.
polarity	Configures the 1PPS polarity.
negative	Configures the polarity as negative. Default polarity is positive.

Command Default

No default behavior or values.

Command Modes

GNSS configuration (config-gnss)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers.

Usage Guidelines

The pulse per second is used to synchronize time with other sensors and is crucial for the accuracy of the sensor integration.

Examples

The following example shows how to configure the PPS:

```
Router# configure terminal
Router(config)# gnss slot r0
Router(config-gnss)# 1pps polarity negative
```

Related Commands

Command	Description
gnss	Configures the GNSS on the router.
anti-jam	Enables or disables the anti-jam mode on the GNSS module.
constellation	Configures the GNSS module based on the specified satellite constellations.
default	Resets the device to its default state.
exit	Exists the GNSS sub mode.
no	Negates the command or sets the value of the command to its default values.
shutdown	Enables GNSS module.

ais-core-failure

To enable AIS alarms to detect core failure events on a 8/16 T1E1 IM, use the ais-core-failure command in controller configuration mode. To disable the AIS alarms, use the no form of this command..

ais-core-failure

no ais-core-failure

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; AIS alarm is not reported during core failure events.

Command Modes

Controller configuration

Command History

Release	Modification
IOS XE Everest 16.7.1	Support for this command was introduced on the Cisco ASR 900 Routers.

Usage Guidelines

AIS alarms are generated and detected either when the TDM circuits goes down on the access layer of the network topology or a failure occurs in the MPLS domain due to which SAToP connectivity goes down. This alarm is only applicable for SDH-E1 and unframed (SAToP) type and is not applicable for framed (CESoP) type.

You cannot configure AIS alarms if CEM group is enabled.You must first remove the CEM group configuration and then configure AIS alarms.

Examples

The following example shows the configuration of AIS alarm:

```
Router> enable
Router#configure terminal
Router(config)#controller t1 0/1/2
Router(config-controller)#ais-core-failure
```

Related Commands

Command	Description
show run | sec	Displays the AIS alarm configuration.

ais-shut

To enable automatic insertion of a Line Alarm Indication Signal (LAIS) in the sent SONET signal whenever the SONET port enters the administrative shutdown state, use the **ais-shut** command in SONET configuration mode. To disable automatic insertion of a LAIS, use the **no** form of this command..

ais-shut

no ais-shut

Syntax Description

Syntax Description

This command has no keywords or arguments.

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

When the line is placed in administrative shutdown state, use the **ais-shut** command to send a signal to downstream equipment that indicates that there is a problem with the line.

Examples

The following example shows the configuration of AIS SHUT:

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

Related Commands

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

alarm-interface

To enter alarm-interface mode and configure the alarm interface controller (AIC), use the **alarm-interface** command in global configuration mode. To leave alarm-interface mode, use the **exit** command.

alarm-interface *slot-number*

Syntax Description

slot-number	Number of the port in which the AIC is installed.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XG	This command was introduced for the Cisco 2600 series and the Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples

The following examples show how the **alarm-interface** command is used in conjunction with the **ipaddress** and the **reset** commands:

```
Router(config)# alarm-interface 5
Router(config-aic)# ip address 10.2.130.105
```

A change in the AIC IP configuration might not take effect until the next time the card is started. Use the **reset** command to restart the card, as in the following example:

```
Router(config-aic)# reset
Alarm Interface Card in slot 5 restarted
Router(config-aic)# end
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
reset	Resets the AIC CPU.

alarm-profile

To create an alarm profile for chassis, card or interface module, and port, use the **alarm-profile** command in configuration mode. To delete the alarm profile, use the **no** form of this command.

The alarm profile is associated to an alarm with controller types such as SONET, SDH, DS1, or DS3.

alarm-profile *profile-name* {**chassis** | **card** | **port**}

Syntax Description

Syntax Description

profile-name	The name of the alarm profile. The name should be a string with alpha numeric characters and should not exceed 32 characters.
chassis	Alarm profile created for chassis.
card	Alarm profile created for card.
port	Alarm profile created for port.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.8.1	Support for this command was introduced on ASR 900 Series.

Usage Guidelines

This command is used to create alarm profile for chassis, card, or port in the configuration mode.

Examples

The following example shows how to create an alarm profile for chassis:

```
router(config)#alarm profile CHASSIS chassis
router(config-alarm-profile)#alarm sonet/sdh
router(config-alarm-properties)#SLOF syslog
router(config-alarm-properties)#SLOF severity critical
```

Examples

The following example shows how to create an alarm profile for card:

```
 router(config)#alarm profile CARD card
router(config-alarm-profile)#alarm ds3
router(config-alarm-properties)#DS3_RX_LOS syslog
router(config-alarm-properties)#DS3_RX_LOS severity major
```

Examples

The following example shows how to create an alarm profile for port:

```
 router(config)#alarm profile PORT port
router(config-alarm-profile)#alarm ds1
router(config-alarm-properties)#DS1_LOS syslog
router(config-alarm-properties)#DS1_LOS severity major
```

Related Commands

Command	Description
alarm-profile *name***attach**	Attaches alarm profile to chassis or card.
attach profile *profile-name*	Attaches alarm profile to port.
show alarm-profile	Displays alarm profile configured for chassis.

alarm-profile attach

To attach an alarm profile to chassis or card, use the **alarm-profile** *name* **attach** command in configuration mode. To detach the alarm profile from chassis or card, use the **no** form of this command.

After attaching the alarm profile only, the alarm serverity and other alarm functionalities are applied to the chassis, card, or port.

alarm-profile *profile-name* attach {**chassis** | **card** *slot/bay*}

alarm-profile *telcordia* **attachchassis**

Syntax Description

Syntax Description

profile-name	The name of the alarm profile.
chassis	Specify to attach the alarm profile to chassis.
card *slot/bay*	Specify to attach the alarm profile to card.
telcordia	Specify to attach the Telcordia alarm profile to chassis.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.8.1	Support for this command was introduced on ASR 900 Series.
Cisco IOS XE 17.3.1	Support for attaching the Telcordia alarm profile to chassis was introduced.

Usage Guidelines

This command is used to attach alarm profile to chassis or card in the configuration mode.

For Telcordia alarm profile, the alarm severities Not Alarmed (NA) and Not Reported (NR) are included by default. The alarm profile attached to chassis inherits the alarm severities of the Telcordia profile.

Note Ensure that you use the complete **alarm-profile telcordia attach chassis** command while attaching the alarm profile based on Telcordia.

Examples

The following example shows how to attach an alarm profile for chassis:

```
 router>enable
router#configure terminal
router(config)#alarm-profile CHASSIS attach chassis
router(config)#end
```

Examples

The following example shows how to attach a Telcordia alarm profile to chassis:

```
 router>enable
router#configure terminal
router(config)#alarm-profile telcordia attach chassis
router(config)#end
```

Examples

The following example shows how to attach an alarm profile to card:

```
 router>enable
router#configure terminal
router(config)#alarm-profile CARD attach card 0/1
router(config)#end
```

Related Commands

Command	Description
alarm-profile *profile-name*	Creates a new alarm profile for chassis, card or port.
show alarm-profile	Displays alarm profile configured for chassis.

alarm report all

To permit selected SONET alarms to be logged to the console for a SONET controller, use the **alarm report all** command in SONET configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

alarm-report all {*b1-tca* | *lias* | *lrdi* | *pais* | *plop* | *pplm* | *pplm* | *prdi* | *sd-ber*}

Syntax Description

Syntax Description

b1-tca	The name of a CEM interface parameters class.
lias	Reports Line Alarm Indication signal (LAIS) errors.
lrdi	Reports line remote defect indication errors.
pais	Enables reporting of Path Alarm Indication Signal (PAIS).
plop	Enables reporting of Path Loss Of Pointer (PLOP).
pplm	Sets Path Payload Mismatch (PPLM) defect reporting status.
prdi	Sets Path Remote Defect Indication (PRDI) reporting status.
sd-ber	Enables Signal Degrade (SD) Bit Error Rate (BER) reporting.

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

This command is used to configure the alarm reports in SONET mode.

Examples

The following example shows the configuration of alarm reports:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
alarm report all b1-tcs
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.

Command	Description
show controller sonet	Displays SONET controller configuration.

als

To enable the Automatic Laser Shutdown (ALS) mode, use the **als**command in interface configuration mode. To disable ALS mode, use the no form of this command.

als
no als

Syntax Description

This command has no arguments or keywords.

Command Default

ALS is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Examples

The following example shows how to enable ALS:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
```

Related Commands

Command	Description
als restart	Requests an ALS restart mode.
als restart mode	Selects the ALS restart mode.
als restart pulse	Select the ALS pulse mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

als restart

To request an Automatic Laser Shutdown (ALS) restart mode, use the **alsrestart**command in interface configuration mode. To disable an ALS restart mode, use the no form of this command.

als restart {**mode** | **pulse**}
no als restart {**mode** | **pulse**}

Syntax Description

mode	Specifies the ALS mode.
pulse	Specifies the ALS pulse.

Command Default

Command default is automatic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Examples

The following example restarts the ALS mode:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart mode	Selects the ALS restart mode.
als restart pulse	Selects the ALS pulse mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

als restart mode

To select the Automatic Laser Shutdown (ALS) restart mode, use the **alsrestartmode**command in interface configuration mode. To reset to the command default mode, use the no form of this command.

als restart mode {**automatic** | **manual**}
no als restart mode {**automatic** | **manual**}

Syntax Description

automatic	Selects automatic mode.
manual	Selects manual mode.

Command Default

Command default is automatic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Usage Guidelines

In manual restart, you request a single restart pulse from the ALS agent. In automatic restart, you configure the ALS agent to send a periodic restart pulse.

Examples

The following example shows how to select automatic mode:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode automatic
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart	Requests an ALS restart mode.
als restart pulse	Select the ALS pulse mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

als restart pulse

To select the Automatic Laser Shutdown (ALS) pulse mode, use the **alsrestartpulse**command in inteface configuration mode. To disable an ALS pulse mode, use the no form of this command.

als restart pulse {**interval seconds** | **width seconds**}
no als restart pulse {**interval seconds** | **width seconds**}

Syntax Description

interval **seconds**	Specifies the interval of the ALS pulse. The range is 100 to 20,000 seconds. Default is 300 seconds.
width seconds	Specifies the width of the ALS pulse. The range is 2 to 200 seconds. Default is 200 seconds.

Command Default

Pulse interval default is 300 seconds. Pulse width default is 200 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router for the ES+ line cards.

Usage Guidelines

If a particular platform/OS/interface/controller has the capability to support two ranges, one range for Wave Division Multiplexing (WDM) and another for non-WDM, use the following pulse width ranges:

- WDM: 60 - 200 (default: 100)
- Non-WDM: 2 - 100 (default: 4)

The recovery pulse interval is the period between the rising edge of pulses. The pulse interval needs to be greater than the pulse width. If a particular platform/OS/interface/controller has the capability to support two ranges, one range for WDM and another for non-WDM, use the following pulse width ranges:

- WDM: 200 - 20000 (default: 300)
- Non-WDM: 100 - 2000 (default: 100)

Examples

The following example shows how to select an ALS pulse interval:

```
Router> enable
Router# configure terminal
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode
Router(config-if)# als restart mode automatic
Router(config-if)# als restart pulse interval 2000
```

The following example shows how to select an ALS pulse width:

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface tengigabitethernet 2/1
Router(config-if)# als
Router(config-if)# als restart mode
Router(config-if)# als restart mode automatic
Router(config-if)# als restart pulse width 200
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart	Requests an ALS restart mode.
als restart mode	Selects the ALS restart mode.
hw-module als restart	Requests a restart pulse.
show als	Displays ALS status.

analysis-module monitoring

To enable Network Analysis Module (NAM) packet monitoring on an interface, use the **analysis-modulemonitoring** command in interface configuration mode. To disable NAM packet monitoring, use the **no** form of this command.

analysis-modulemonitoring
noanalysis-modulemonitoring

Syntax Description

This command has no arguments or keywords.

Command Default

NAM packet monitoring is disabled on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, Cisco 2851, and Cisco 3800 series.
12.3(11)T	This command was implemented on the Cisco 3800 series.
Cisco IOS XE Fuji 16.9.1	This command was implemented on the Cisco ISR 4000 Series Integrated Services Routers.

Usage Guidelines

When you enable NAM packet monitoring on an interface, Cisco Express Forwarding (CEF) sends an extra copy of IP packet that is received or sent on that interface to the NAM through the analysis module and then through the internal NM-NAM interface.

Note The traffic is sent through the internal NAM interface and through the the analysis module interface uses the router's resources such as CPU, SDRAM bandwidth, and backplane Peripheral Component Interconnect (PCI) bandwidth. Therefore, it is recommended to use the internal NAM interface to monitor WAN interfaces and use the external NAM interface to monitor LAN interfaces.

In Cisco IOS XE Fuji 16.9.1, Encapsulated Remote Switched Port Analyzer (ERSPAN) supports the NAM feature on Cisco 4000 Series ISRs. The Cisco ERSPAN feature allows you to monitor traffic on one or more ports and then sends the monitored traffic to one or more destination ports.

To enhance the performance of NAM and simplify the configuration of NAM data port, ERSPAN sessions are extended to a special souce session called NAM SPAN. NAM SPAN supports Layer 2 mode as local span and monitors the interface on Layer 3 interface on Cisco 4000 Series ISRs.

Note If an interface is monitored by NAM SPAN, it can not be configured as output interface. Each interface can configure only one interface as output interface.

Examples

The following example shows how to enable NAM packet monitoring on a serial interface:

```
Router(config)# interface serial 0/0
Router(config-if)# analysis-module monitoring
```

The following example shows how to enable NAM packet monitoring on a serial interface of a Cisco 4000 Series ISRs:

```
Router(config)# interface serial 0/0
Router(config-if)# analysis-module monitoring ucse0/0/0
```

Note The output interface is ucse0/0/0 which is configured as NAM/vNAM data port and the source interface is serial 0/0 in this example.

announce interval

To set an interval value for timing announcement packets, use the **announceinterval** command in Precision Time Protocol clock port mode. To remove an announcement interval configuration, use the **no** form of this command.

announce interval *interval-value*
no announce interval *interval-value*

Syntax Description

interval-value	Specifies the interval for announce messages. The intervals use log base 2 values, as follows: • 4--1 packet every 16 seconds • 3--1 packet every 8 seconds • 2--1 packet every 4 seconds • 1--1 packet every 2 seconds • 0--1 packet every second

Command Default

For the IE 3000 switch, the default value is 1. For the MWR 2941 router, the default value is 2.

Command Modes

PTP clock port configuration (config-ptp-port)

Command History

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

Usage Guidelines

The interval value defined by this command impacts the timeout value defined by the **announcetimeout** command.

Examples

The following example shows how to configure an announcement interval:

```
Router# configure terminal
Router(config)# ptp clock ordinary domain 0
Router(config-ptp-clk)# clock-port slave slaveport
Router(config-ptp-port)# announce interval 3
Router(config-ptp-port)# end
```

Related Commands

Command	Description
announce timeout	Sets the timeout value for timing announcement packets.

announce timeout

To set a timeout value for timing announcement packets, use the **announcetimeout** command in Precision Time Protocol clock port mode. To remove an announcement timeout configuration, use the **no** form of this command.

announce timeout *timeout-value*
no announce timeout *timeout-value*

Syntax Description

timeout-value	Specifies the number of announcement intervals before the session times out. The range is from 1 to 10. The default is 3.

Command Default

The default timeout value is 3.

Command Modes

PTP clock port configuration (config-ptp-port)

Command History

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

Usage Guidelines

This command configures the number of announcement intervals before the session times out. To define the length of the announcement intervals, use the **announceinterval** command.

Examples

The following example shows how to configure an **announcementtimeout**:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# clock-port slave slaveport
Device(config-ptp-port)# announce timeout 7
Device(config-ptp-port)# end
```

Related Commands

Command	Description
announce interval	Sets interval value for timing announcement packets.

anti-jam

To configure the anti-jam mode for the GNSS module on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers, use the **anti-jam** command in gnss mode.

anti-jam disable

Syntax Description

disable	Disables the anti-jam mode.

Command Default

Anti-jam is enabled on the GNSS module by default.

Command Modes

GNSS configuration (config-gnss)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers.

Examples

The following example shows how to disable the anti-jam mode on the GNSS module:

```
Router# configure terminal
Router(config)# gnss slot r0
Router(config-gnss)# anti-jam disable
```

Related Commands

Command	Description
gnss	Configures the GNSS on the router.
1pps	Configures the pulse per second from the GNSS module.
constellation	Configures the GNSS module based on the specified satellite constellations.
default	Resets the device to its default state.
exit	Exists the GNSS sub mode.

apply (satellite initial configuration)

To save new or changed satellite initial configuration parameters and to reset the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **apply** command in satellite initial configuration mode.

apply

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration mode

Command History

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

Usage Guidelines

The **apply** command saves any new or changed satellite initial configuration parameters to the nonvolatile memory of the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT) and initiates a network module software reset. Commands entered in satellite initial configuration mode do not appear in the router configuration.

When you enter the **exit** or **end** command to exit satellite initial configuration mode, the system automatically saves any changed parameters to the NM-1VSAT-GILAT network module's nonvolatile memory and resets the NM-1VSAT-GILAT network module.

Note 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 what appears when you enter the **apply** command after changing some initial configuration parameters:

```
Router(sat-init-config)# apply

Applying changed parameters to the satellite module.
Parameter update succeeded.  Module is now resetting.
Router(sat-init-config)#
```

The following example shows what appears when you enter the **apply** command when no parameters have been changed:

```
Router(sat-init-config)# apply

% No new or changed parameters to apply.
Router(sat-init-config)#
```

Related Commands

Command	Description
end (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
exit (satellite initial configuration)	Exits satellite initial configuration mode, saves any new or changed parameters, and resets the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

aps authenticate

To enable authentication and specify the string that must be present to accept any packet on the out-of-band (OOB) communications channel on a Packet-over-SONET (POS) interface, use the **apsauthenticate** command in interface configuration mode. To disable authentication, use the **no** form of this command.

aps authenticate *string*
no aps authenticate

Syntax Description

string	Text that must be present to accept the packet on a protected or working interface. A maximum of eight alphanumeric characters are accepted.

Command Default

Authentication is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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 the **apsauthenticate**command to ensure that only valid packets are accepted on the OOB communications channel.

The **apsauthenticate** command must be configured on both the working and protect interfaces.

Examples

The following example shows how to enable authentication on POS interface 0 in slot 4:

```
Router# configure terminal
Router(config)# interface pos 4/0/0
Router(config-if)# aps working 1
Router(config-if)# aps authenticate sanjose
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps adm

Use this command to configure unidirectional ACR (SONET Framing).

aps adm *slot* / *bay* / *port*

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.

Usage Guidelines

The command is used to enable Add Drop Multiplexer (ADM) with unidirectional APS protection.

Examples

The following example shows how to configure unidirectional ACR (SONET Framing):

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
clock source internal
aps group acr 1
aps working 1
aps unidirectional
aps adm
exit
controller sonet 0/5/0
aps group acr 1
aps protect 1 10.7.7.7
aps revert 3
end
```

Related Commands

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

aps clear sonet

To remove all externally initiated SONET automatic protection switching (APS) commands configured on a Cisco AS5850, use the **apsclearsonet**command in privileged EXEC mode.

aps clear sonet *slot*/*port*

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.

Command Default

No APS switch commands are removed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Use the **apsclearsonet**command to remove any SONET APS commands, such as the **apsforcesonet**command, that could switch the working fiber to the protect fiber on an STM-1 trunk card.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to remove all externally initiated SONET APS switch commands:

```
Router# aps clear sonet 1/0
```

Related Commands

Command	Description
aps force sonet	Requests an APS forced switch of a specified port to the alternate port unless a request of equal or higher priority is in effect.
aps lockout sonet	Prevents a working SONET port from switching to a protect SONET port unless a request of equal or higher priority is in effect.
aps manual sonet	Requests a manual APS switch on a SONET port.
aps protect (SONET)	Enables SONET APS.

aps force

To manually switch the specified circuit to a protect interface, unless a request of equal or higher priority is in effect, use the **apsforce**command in interface configuration mode. To cancel the switch, use the **no** form of this command.

aps force *circuit-number*
no aps force *circuit-number*

Syntax Description

circuit-number	Number of the circuit to switch to the protect interface.

Command Default

No circuit is switched.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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 the **apsforce**command to manually switch the interface to a protect interface when you are not using the **apsrevert**command. For example, if you need to change the fiber connection, you can manually force the working interface to switch to the protect interface.

In a one-plus-one (1+1) configuration only, you can use the **apsforce0** command to force traffic from the protect interface back onto the working interface.

The**apsforce** command has a higher priority than any of the signal failures or the **apsmanual** command.

The **apsforce** command is configured only on protect interfaces.

Examples

The following example shows how to force the circuit on POS interface 0 in slot 3 (a protect interface) back onto a working interface:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps protect 10/30/1/1
Router(config-if)# aps force 1
Router(config-if)# end
```

Related Commands

Command	Description
aps manual	Manually switches a circuit to a protect interface.
aps protect	Enables a POS interface as a protect interface.

Command	Description
aps working	Configures a POS interface as a working interface.

aps force sonet

To force a specified port to switch to the alternate port within a redundant pair unless a request of equal or higher priority is in effect, use the **apsforcesonet**command in privileged EXEC mode.

aps force sonet *slot*/*port* **from** {**protection** | **working**}

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.
from protection	Specifies that you want to switch from the protect port to the working port.
from working	Specifies that you want to switch from the working port to the protect port.

Command Default

No port is switched.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Forced is a defined APS request priority level. The request succeeds if no higher priority request (lockout is the only higher priority request) is posted. The **apsforcesonet**command does not persist after a system restart. The *slot* and *port* arguments indicate the SONET interface on which you want to issue the **apsforcesonet** command. The**apsforcesonet** command has a higher priority than any of the signal failures or the **apsmanualsonet** command.

For more information about APS priority requests, see the ITU-T G.841 standard.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to force the protect port in the SONET controller to become an active port:

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
Router# aps force sonet 1/0 from working
```

Related Commands

Command	Description
aps clear sonet	Removes any APS switch commands configured using CLI.
aps lockout sonet	Prevents a working SONET port from switching to a protect SONET port unless a request of equal or higher priority is in effect.

Command	Description
aps manual sonet	Requests a manual APS switch on a SONET port.
aps protect (SONET)	Enables SONET APS.

aps group

To allow more than one protect and working interface and Access Circuit Redundancy (ACR) group to be supported on a router, use the **aps group** command in interface configuration or controller configuration mode. To remove a group, use the **no** form of this command.

aps group [**acr**] *group-number*
no aps group [**acr**] *group-number*

Syntax Description

acr	(Optional) Specifies an ACR group.
group-number	Number of the group. The default is 0.

Command Default

No groups exist.

Note 0 is a valid group number.

Command Modes

Interface configuration (config-if)
Controller configuration (config-controller)

Command History

Release	Modification
11.1CC	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.
15.1(1)S	This command was modified. The **acr** keyword was added.

Usage Guidelines

Use the **aps group**command to specify more than one working and protect interface on a router--for example, working channel for group 0 and protect channel for group 1 on one router, and working channel for group 1 and protect channel for group 0 on another router.

The default group number is 0. The **aps group 0** command does not imply that no groups exist.

The **aps group** command must be configured on both the protect and working interfaces.

Use the **acr**keyword to configure an ACR working or protect interface.

Examples

The following example shows how to configure two working/protect interface pairs. Working interface (3/0/0) is configured in group 10 (the protect interface for this working interface is configured on another router), and protect interface (2/0/1) is configured in group 20.

```
Router# configure terminal
```

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip address 10.7.7.6 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 3/0/0
Router(config-if)# aps group 10
Router(config-if)# aps working 1
Router(config-if)# exit
Router(config)# interface pos 2/0/1
Router(config-if)# aps group 20
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

On the second router, protect interface (4/0/0) is configured in group 10, and working interface (5/0/0) is configured in group 20 (the protect interface for this working interface is configured on another router).

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip address 10.7.7.7 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 4/0/0
Router(config-if)# aps group 10
Router(config-if)# aps protect 1 10.7.7.6
Router(config-if)# exit
Router(config)# interface pos 5/0/0
Router(config-if)# aps group 20
Router(config-if)# aps working 1
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps hspw-icrm-grp

To associate an Automatic Protection Switching (APS) group to an Interchassis Redundancy Manager (ICRM) group number, use the **aps hspw-icrm-grp** command in controller configuration mode. To remove the association, use the **no** form of this command.

aps hspw-icrm-grp *group-number*
no aps hspw-icrm-grp *group-number*

Syntax Description

group-number	ICRM group number. Valid values are from 1 to 4294967295.

Command Default

Interface connections do not switch from one circuit to another if a circuit fails.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
Cisco IOS 15.2(1)S	This command was introduced.
Cisco IOS XE 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **aps hspw-icrm-grp** command to protect SONET networks by enabling SONET connections to switch to another SONET circuit when a circuit failure occurs.

A protect interface serves as the backup interface for the working interface. When the working interface fails, the protect interface quickly assumes the former's traffic load.

Examples

The following example shows how to configure the Multi Router Automatic Protection Switching (MR-APS) integration with HSPW on a Circuit Emulation (CEM) interface on the working router with framing mode as SONET on router P1:

```
RouterP1> enable
RouterP1# configure terminal
RouterP1(config)# pseudowire-class hspw_aps
RouterP1(config-pw-class)# encapsulation mpls
RouterP1(config-pw-class)# status peer topology dual-homed
RouterP1(config-pw-class)# exit
RouterP1(config)# redundancy
RouterP1(config-red)# interchassis group 1
RouterP1(config-r-ic)# member ip 10.2.0.2
RouterP1(config-r-ic)# backbone interface GigabitEthernet 0/1/0
RouterP1(config-r-ic)# backbone interface GigabitEthernet 0/1/1
RouterP1(config-r-ic)# exit
RouterP1(config)# controller SONET 0/1/0
RouterP1(config-controller)# framing sonet
RouterP1(config-controller)# clock source line
RouterP1(config-controller)# sts-1 1
RouterP1(config-ctrlr-sts1)# mode vt-15
RouterP1(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterP1(config-ctrlr-sts1)# exit
RouterP1(config-controller)# aps group 3
RouterP1(config-controller)# aps working 1
```

```
RouterP1(config-controller)# aps hspw-icrm-grp 1
RouterP1(config-controller)# exit
RouterP1(config)# interface cem 0/1/0
RouterP1(config-if)# cem 0
RouterP1(config-if)# xconnect 3.3.3.3 1 encapsulation mpls pw-class hspw_aps
RouterP1(config-if)# backup peer 4.4.4.4 2 pw-class hspw_aps
RouterP1(config-if)# exit
RouterP1(config)# end
```

Examples

The following example shows how to configure the MR-APS integration with hot standby pseudowire (HSPW) on a CEM interface on the protect router with framing mode as SONET on router PE1:

```
RouterPE1> enable
RouterPE1# configure terminal
RouterPE1(config)# pseudowire-class hspw_aps
RouterPE1(config-pw-class)# encapsulation mpls
RouterPE1(config-pw-class)# status peer topology dual-homed
RouterPE1(config-pw-class)# exit
RouterPE1(config)# redundancy
RouterPE1(config-red)# interchassis group 1
RouterPE1(config-r-ic)# member ip 10.2.0.1
RouterPE1(config-r-ic)# backbone interface GigabitEthernet 0/1/0
RouterPE1(config-r-ic)# backbone interface GigabitEthernet 0/1/1
RouterPE1(config-r-ic)# exit
RouterPE1(config)# controller SONET 0/2/0
RouterPE1(config-controller)# framing sonet
RouterPE1(config-controller)# clock source line
RouterPE1(config-controller)# sts-1 1
RouterPE1(config-ctrlr-sts1)# mode vt-15
RouterPE1(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterPE1(config-ctrlr-sts1)# exit
RouterPE1(config-controller)# aps group 3
RouterPE1(config-controller)# aps protect 1 10.2.0.1
RouterPE1(config-controller)# aps hspw-icrm-grp 1
RouterPE1(config-controller)# exit
RouterPE1(config)# interface cem 0/2/0
RouterPE1(config-if)# cem 0
RouterPE1(config-if)# xconnect 3.3.3.3 3 pw-class hspw_aps
RouterPE1(config-if)# backup peer 4.4.4.4 4 pw-class hspw_aps
RouterPE1(config-if)# exit
RouterPE1(config)# end
```

Examples

The following example shows how to configure the MR-APS integration with HSPW on a CEM interface on the working router with framing mode as SONET on router P2:

```
RouterP2> enable
RouterP2# configure terminal
RouterP2(config)# pseudowire-class hspw_aps
RouterP2(config-pw-class)# encapsulation mpls
RouterP2(config-pw-class)# status peer topology dual-homed
RouterP2(config-pw-class)# exit
RouterP2(config)# redundancy
RouterP2(config-red)# interchassis group 1
RouterP2(config-r-ic)# member ip 10.6.0.2
RouterP2(config-r-ic)# backbone interface GigabitEthernet 0/2/0
RouterP2(config-r-ic)# backbone interface GigabitEthernet 0/2/1
RouterP2(config-r-ic)# exit
RouterP2(config)# controller SONET 0/1/0
RouterP2(config-controller)# framing sonet
```

```
RouterP2(config-controller)# clock source line
RouterP2(config-controller)# sts-1 1
RouterP2(config-ctrlr-sts1)# mode vt-15
RouterP2(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterP2(config-ctrlr-sts1)# exit
RouterP2(config-controller)# aps group 3
RouterP2(config-controller)# aps working 1
RouterP2(config-controller)# aps hspw-icrm-grp 1
RouterP2(config-controller)# exit
RouterP2(config)# interface cem 0/1/0
RouterP2(config-if)# cem 0
RouterP2(config-if)# xconnect 1.1.1.1 1 encapsulation mpls pw-class hspw_aps
RouterP2(config-if)# backup peer 2.2.2.2 3 pw-class hspw_aps
RouterP2(config-if)# exit
RouterP2(config)# end
```

Examples

The following example shows how to configure the MR-APS Integration with HSPW on a CEM interface on the protect router with framing mode as SONET on router PE2:

```
RouterPE2> enable
RouterPE2# configure terminal
RouterPE2(config)# pseudowire-class hspw_aps
RouterPE2(config-pw-class)# encapsulation mpls
RouterPE2(config-pw-class)# status peer topology dual-homed
RouterPE2(config-pw-class)# exit
RouterPE2(config)# redundancy
RouterPE2(config-red)# interchassis group 1
RouterPE2(config-r-ic)# member ip 10.6.0.1
RouterPE2(config-r-ic)# backbone interface GigabitEthernet 0/2/0
RouterPE2(config-r-ic)# backbone interface GigabitEthernet 0/2/1
RouterPE2(config-r-ic)# exit
RouterPE2(config)# controller SONET 0/2/0
RouterPE2(config-controller)# framing sonet
RouterPE2(config-controller)# clock source line
RouterPE2(config-controller)# sts-1 1
RouterPE2(config-ctrlr-sts1)# mode vt-15
RouterPE2(config-ctrlr-sts1)# vtg 1 t1 1 cem-group 0 timeslots 1-24
RouterPE2(config-ctrlr-sts1)# exit
RouterPE2(config-controller)# aps group 2
RouterPE2(config-controller)# aps protect 1 10.6.0.1
RouterPE2(config-controller)# aps hspw-icrm-grp 1
RouterPE2(config-controller)# exit
RouterPE2(config)# interface cem 0/2/0
RouterPE2(config-if)# cem 0
RouterPE2(config-if)# xconnect 1.1.1.1 2 pw-class hspw_aps
RouterPE2(config-if)# backup peer 2.2.2.2 4 pw-class hspw_aps
RouterPE2(config-if)# exit
```

Related Commands

Command	Description
aps protect	Configures a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps lockout

To prevent a working interface from switching to a protect interface, use the **apslockout** command in interface configuration mode. To remove the lockout, use the **no** form of this command.

aps lockout *circuit-number*
no aps lockout *circuit-number*

Syntax Description

circuit-number	Number of the circuit to lock out.

Command Default

No lockout exists.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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 **apslockout** command is configured only on protect interfaces.

Examples

The following example shows how to lock out POS interface 3/0/0 (that is, prevents the circuit from switching to a protect interface if the working circuit becomes unavailable):

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# aps lockout 1
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps lockout sonet

To prevent a working port from switching to a protect port unless a request of equal or higher priority is in effect, use the **apslockoutsonet** command in privileged EXEC mode.

aps lockout sonet *slot*/*port*

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.

Command Default

No lockout exists; that is, a working port is not prevented from switching to a protect port.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Lockout is defined as the highest APS request priority level.

The **apslockoutsonet**command does not persist after a system restart. The *slot* and *port* arguments indicate the SONET interface from which the protect port is to be locked out. When the specified port is locked out, SONET APS switching from the working port is not allowed.

For more information about APS priority requests, see the ITU-T G.841 standard.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to lock out SONET port 1/0 (prevents SONET APS switching to a protect interface if the working circuit becomes unavailable):

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
Router# aps lockout sonet 1/0
```

Related Commands

Command	Description
aps clear sonet	Removes any APS switch commands configured using CLI.
aps force sonet	Requests an APS forced switch of a specified port to the alternate port unless a request of equal or higher priority is in effect.
aps manual sonet	Requests a manual APS switch on a SONET port.
aps protect (SONET)	Enables SONET APS.

aps manual

To manually switch a circuit to a protect interface, use the **aps manual** command in interface configuration mode. To cancel the switch, use the **no** form of this command.

aps manual *circuit-number*
no aps manual *circuit-number*

Syntax Description

circuit-number	Number of the circuit to switch to a protect interface.

Command Default

No circuit is switched.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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 the **aps manual** command to manually switch the interface to a protect interface. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **aps manual** command to revert the communication link back to the working interface before the wait to restore (WTR) time has expired. The WTR time period is set by the **aps revert** command.

In a one-plus-one (1+1) configuration only, you can use the **aps manual 0** command to force traffic from the protect interface back onto the working interface.

The**aps manual** command is a lower priority than any of the signal failures or the**aps force** command.

Examples

The following example shows how to force the circuit on POS interface 0 in slot 3 (a working interface) back onto the protect interface:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps working 1
Router(config-if)# aps manual 1
Router(config-if)# end
```

Related Commands

Command	Description
aps force	Manually switches the specified circuit to a protect interface, unless a request of equal or higher priority is in effect.
aps protect	Enables a POS interface as a protect interface.

Command	Description
aps revert	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
aps working	Configures a POS interface as a working interface.

aps manual sonet

To manually switch to the alternate port within a redundant pair unless a request of equal or higher priority is in effect, use the **apsmanualsonet** command in privileged EXEC mode.

aps manual sonet *slot*/*port* **from** {**protection** | **working**}

Syntax Description

slot	Slot number on an STM-1 trunk card.
/ *port*	SONET port number on an STM-1 trunk card. The slash mark is required between the *slot* argument and the *port* argument.
from protection	Specifies that you want to switch from the protect port to the working port.
from working	Specifies that you want to switch from the working port to the protect port.

Command Default

No port is switched.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Use the **apsmanualsonet**command to manually switch the active port to the alternate port. For example, you can use this command when you need to perform maintenance on the working port.

Manual is a defined APS request priority level. The request succeeds if no higher priority request is posted. The **apsmanualsonet**command does not persist after a system restart. The *slot* and *port* arguments indicate the SONET interface on which you want to issue the **apsmanualsonet** command. The**apsmanualsonet** command has a lower priority than any of the signal failures or the **apsforcesonet**command.

For more information about APS priority requests, see the ITU-T G.841 standard.

This command applies to the Cisco AS5850 universal gateway only.

Examples

The following example shows how to manually switch the working port, SONET port 1/0, to the protect port:

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
Router# aps manual sonet 1/0 from working
```

Related Commands

Command	Description
aps clear sonet	Removes any APS switch commands configured using CLI.

Command	Description
aps force sonet	Requests an APS forced switch of a specified port to the alternate port unless a request of equal or higher priority is in effect.
aps lockout sonet	Prevents a working SONET port from switching to a protect SONET port unless a request of equal or higher priority is in effect.
aps protect (SONET)	Enables SONET APS.

aps protect

To enable a POS interface as a protect interface, use the **apsprotect**command in interface configuration mode. To remove the POS interface as a protect interface, use the **no** form of this command.

aps protect *circuit-number ip-address*
no aps protect *circuit-number ip-address*

Syntax Description

circuit-number	Number of the circuit to enable as a protect interface.
ip-address	IP address of the router that has the working POS interface.

Command Default

No circuit is protected.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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 the **apsprotect**command to configure the POS interface used by a working interface if the working interface becomes unavailable because of a router failure, degradation or loss of channel signal, or manual intervention.



Caution Configure the working interface before configuring the protect interface to keep the protect interface from becoming the active circuit and disabling the working circuit when it is finally discovered.

Examples

The following example shows how to configure circuit 1 on POS interface 5/0/0 as a protect interface for the working interface on the router with the IP address of 10.7.7.7. For information on how to configure the working interface, refer to the **apsworking** command.

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

Related Commands

Command	Description
aps working	Configures a POS interface as a working interface.

aps protect (SONET)

To enable automatic protection switching (APS) on a SONET port in an STM-1 trunk card, use the **apsprotect**command in controller configuration mode. To disable APS on the SONET port, use the **no** form of this command.

aps protect
no aps protect

Syntax Description

This command has no arguments or keywords.

Command Default

APS is disabled.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(11)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Use the **apsprotect**command to enable APS on a protect SONET port as a working port if the working port becomes unavailable because of a fiber failure, degradation or loss of channel signal, or manual intervention.

Examples

The following example shows how to enable APS on SONET port 0/1 in an STM-1 trunk card.

```
Router# configure terminal
Router(config)# controller sonet 1/0
Router(config-controller)# aps protect
Router(config-controller)# end
```

Related Commands

Command	Description
aps unidirectional	Configures a protect SONET port for unidirectional mode.
show controllers sonet	Displays information about SONET controllers.

aps revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **apsrevert**command in interface configuration mode. To disable automatic switchover, use the **no** form of this command.

aps revert *minutes*
no aps revert

Syntax Description

minutes	Number of minutes until the circuit is switched back to the working interface after the working interface is available.

Command Default

Automatic switchover is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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 the **apsrevert**command to return the circuit to the working interface when it becomes available.

The **apsrevert** command is configured only on protect interfaces.

Examples

The following example shows how to enable circuit 1 on POS interface 5/0/0 to revert to the working interface after the working interface has been available for 3 minutes:

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# aps revert 3
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.

aps timers

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **apstimers**command in interface configuration mode. To return to the default timers, use the **no** form of this command.

aps timers *seconds1 seconds2*
no aps timers

Syntax Description

seconds1	Number of seconds to wait before sending a hello packet (hello timer). Default is 1.
seconds2	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer). Default is 3.

Command Default

Hello time is 1 second Hold time is 3 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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 the **apstimers**command to control the time between an automatic switchover from the protect interface to the working interface after the working interface becomes available.

Normally, the hold time is greater than or equal to three times the hello time.

The **apstimers** command is configured only on protect interfaces.

Examples

The following example shows how to specify a hello time of 2 seconds and a hold time of 6 seconds on circuit 1 on POS interface 5/0/0:

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps working 1
Router(config-if)# aps timers 2 6
Router(config-if)# end
```

aps unidirectional

To configure a protect interface for unidirectional mode, use the **apsunidirectional** command in controller configuration or interface configuration mode. To return to the default, bidirectional mode, use the **no** form of this command.

aps unidirectional
no aps unidirectional

Syntax Description

This command has no arguments or keywords.

Command Default

Bidirectional mode

Command Modes

Controller configuration Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.3(11)T	Support for SONET APS using an STM-1 card was added on the Cisco AS5850.
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 **apsunidirectional**command is configured only on protect interfaces.

Use the **apsunidirectional**command when you must interoperate with SONET network equipment, add/drop multiplexors (ADMs) that supports unidirectional mode.

Note We recommend bidirectional mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as bidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. This happens automatically when the SONET network equipment is in bidirectional mode.

Examples

The following example shows how to configure POS interface 3/0/0 for unidirectional mode on a Cisco 12000 series router:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps unidirectional
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

The following example shows how to configure SONET port 0/0 for unidirectional mode on a Cisco AS5850 universal gateway using an STM-1 trunk card:

```
Router# configure terminal
Router(config)# controller sonet 0/0
Router(config-controller)# aps protect
Router(config-controller)# aps unidirectional
Router(config-controller)# end
```

aps working

To configure a Packet over SONET (POS) interface as a working interface, use the **apsworking** command in interface configuration mode. To remove the protect option from the POS interface, use the **no** form of this command.

aps working *circuit-number*
no aps working *circuit-number*

Syntax Description

circuit-number	Circuit number associated with this working interface.

Command Default

No circuit is configured as working.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	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

When a working interface becomes unavailable because of a router failure, degradation or loss of channel signal, or manual intervention, the circuit is switched to the protect interface to maintain the connection.

To enable the circuit on the protect interface to switch back to the working interface after the working interface becomes available again, use the **apsrevert** command in interface configuration mode.

Caution Configure the working interface before configuring the protect interface to keep the protect interface from becoming the active circuit and disabling the working circuit when it is finally discovered.

Examples

The following example shows how to configure POS interface 0 in slot 4 as a working interface. For information on how to configure the protect interface, refer to the **apsprotect** command.

```
Router# configure terminal
Router(config)# interface pos 4/0/0
Router(config-if)# aps working 1
Router(config-if)# end
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.

Command	Description
aps revert	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.

associate slot

To logically associate slots for automatic protection switching (APS) processor redundancy, use the associate slot command in redundancy configuration mode. To disable slot associations, use the no form of this command.

Single Router APS--Cisco 10000 Series Routers and Cisco uBR10012 Universal Broadband Router
associate slot *slot-one* [*slot-two*]
no associate slot *slot-one* [*slot-two*]

Multirouter APS--Cisco 10000 Series Routers
associate slot *slot-one* **mr-aps**
no associate slot *slot-one* **mr-aps**

Syntax Description

slot-one	**Cisco 10000 Series Router** First slot number to be associated for redundancy. Valid range is from 1 to 8. **Cisco uBR10012 Universal Broadband Router** Specifies the slot that contains the working (primary) card. The available range is 1 to 8, but on the Cisco uBR10012 router the only valid numbers are 1 and 3, and the card must support APS redundancy.
slot-two	**Cisco 10000 Series Router** (Optional) Second slot number to be associated for redundancy. Valid range is from 1 to 8. **Cisco uBR10012 Universal Broadband Router** (Optional) Specifies the slot that contains the redundant (backup) card. The available range is 1 to 8, but on the Cisco uBR10012 router the only valid numbers are 2 and 4. If not specified, the next higher adjacent slot is automatically configured as the redundant slot.
mr-aps	(Cisco 10000 Series Routers Only) Specifies that the slot association is between slots in different routers as part of a multirouter APS configuration.

Command Default

No slots are associated.

Command Modes

Redundancy configuration

Command History

Release	Modification
12.1(5a)EY	This command was introduced.
12.0(23)SX	The mr-aps keyword was added to support multirouter APS on the OC3ATM and OC12ATM line cards for the Cisco 10000 series router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S, and support was added for the CHOC12, CHSTM1, OC32POS, and OC12POS line cards for the Cisco 10000 series router.
12.2(4)XF1	This command was introduced for the Cisco uBR10012 router.

Release	Modification
12.2(13)BC1	Support was added for the Cisco OC-48 DPT/POS adapter card on the Cisco uBR10012 router.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA. Support for the Cisco uBR7225VXR router was added.

Usage Guidelines

Cisco 10000 Series Router

Use the **associate** command to associate two cards for single-router APS or multirouter APS redundancy protection. Multirouter APS support is specific to the Cisco 10000 series router. Use the mr-aps keyword in a multirouter APS configuration to allow a protect interface on a second router to be a backup for a working interface on the first router.

The associated slots must use the same type of interface module and must support APS redundancy. The cards also must be located in adjacent slots, for example slots 3 and 4.

Cisco uBR10012 Universal Broadband Router

The two cards must be in adjacent slots, with the working card in slot 1 or 3, and the backup card in slot 2 or 4, respectively. The two cards must be identical cards and must support APS redundancy (such as the OC-12 POS line card).



Note You cannot use the **associate** command with any of the Performance Routing Engine (PRE) modules or TCC+ cards, because these cards are automatically configured for redundant operation when two cards are installed in the chassis.

Examples

Single Router APS Example

The following example shows how to associate two slots in the same router in a single router APS configuration:

```
redundancy
 associate slot 3 4
```

Multirouter APS Example on the Cisco 10000 Series Router Only

The following example shows how to associate two separate slots in different routers in a multirouter APS configuration:

```
! Associate slot 3 on first router for APS redundancy
!
redundancy
 associate slot 3 mr-aps
!
! Associate slot 2 on second router for APS redundancy
```

```
!
redundancy
 associate slot 2 mr-aps
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.

association

To configure an association between current node and a remote node, use the **association** command in interprocess communication (IPC) zone configuration mode. To disable this functionality, use the **no** form of this command.

association *association-ID*
no association *association-ID*

Syntax Description

association-ID	Association ID assignment. The value range is from 1 through 255. The association ID must be unique within a specific zone.

Command Default

No association between a current node and a remote node exists.

Command Modes

IPC zone configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **association** command to configure an association between current node and a remote node. There can be multiple associations within a zone.

Examples

The following example configures an association with an ID of 1:

```
Router(config-ipczone)# association 1
```

Related Commands

Command	Description
ipc zone default	Enters IPC zone configuration mode.
show ipc	Displays IPC statistics.

attach profile-name

To attach alarm profile to port, enter into controller configuration mode, and use the **attach profile-name** command in global configuration mode.

Command to enter into controller configuration mode:

controller {**sonet** | **sdh** | **t1** | **e1** | **t3** | **e3**} *slot*/*bay*/*port*
Command to attach alarm profile to port

`attach`*profile-name*

Syntax Description

sonet	Specifies SONET controller
sdh	Specifies SDH controller
t1	Specifies T1 controller
e1	Specifies E1 controller
slot	Specifies the slot number of the interface.
bay	Specifies the bay number of the interface.
port	Specifies the port number of the interface.
profile-name	Alarm profile to attach to the port.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.8.1	Support for this command was introduced on ASR 900 Series.

Usage Guidelines

Enter into the controller configuration mode and then attach the alarm profile to the interface.

Examples

The following example shows how to configure SONET controller in slot 0, bay 3, port 3 and then attach the alarm profile *PORT* to the interface:

```
Router(config)# controller sonet 0/3/3
Router(config-controller)#attach profile PORT
Router(config-controller)#end
```

Related Commands

Command	Description
alarm-profile *name* **chassis** | **card** | **port**}	Creates new alarm profile for chassis, card, or port.

Command	Description
show alarm-profile	Displays alarm profile configured for chassis.

atm sonet

To set the mode of operation and thus control the type of the ATM cell used for cell-rate decoupling on the SONET physical layer interface module (PLIM), use the **atmsonet**command in interface configuration mode. To restore the default Synchronous Transport Signal level 12, concatenated (STS-12c) operation, use the **no** form of this command.

atm sonet [**stm-4**]
no atm sonet [**stm-4**]

Syntax Description

stm-4	(Optional) Synchronous Digital Hierarchy/Synchronous Transport Signal level 4 (SDH/STM-4) operation (ITU-T specification).

Command Default

STS-12c

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
11.2GS	The **stm-4** 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

Use STM-4 in applications in which SDH framing is required.

Use the default (STS-12c) in applications in which the ATM switch requires “unassigned cells” for rate adaptation. An unassigned cell contains 32 zeros.

Examples

The following example shows how to set the mode of operation to SONET STM-4 on ATM interface 3/0:

```
Router(config)#
 interface atm 3/0
Router(config-if)#
 atm sonet stm-4
Router(config-if)#
 end
```

au-3

To configure a particular Administrative Unit type 3 (AU-3) of an E1 line that has been mapped to an AU-3, use the **au-3**command in controller configuration mode.

au-3 *au-3-number*

Syntax Description

au-3-number	Number in the range from 1 to 3.

Command Default

No default behavior or values

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
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.
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

An administrative unit group (AUG) of an STM-1 can be derived from either AU-3s or an AU-4. Use the **augmappingau-3**configuration controller command to map the AUG to an AU-3 with the following muxing/alignment/mapping:

C-12 <--> VC-12 <--> TU-12 <--> TUG-2 <--> VC-3 <--> AU-3 <--> AUG

Configuring the **au-3**command enables you to enter configuration controller au3 command mode and creates a serial interface with the following name format:

slot/port-adapter/port**.**au-3-number/tug-2-number/e1-number

The aug mapping au-3 and **au-3** commands are available only when Synchronous Digital Hierarchy (SDH) framing is configured.

Examples

The following example shows how to configure AUG mapping to be derived from an AU-3 and selects AU-3 3 to configure as a serial interface:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-3
Router(config-ctrlr-au3)# au-3 3
```

Related Commands

Command	Description
au-4 tug-3	Specifies a TUG-3 for configuration.
aug mapping	Configures the AUG mapping mode of the PA-MC-STM-1 to AU-3.

au-4 tug-3

To specify the Administrative Unit type 4 (AU-4) and Tributary Unit group type 3 (TUG-3) number of an E1 line that has been mapped to an AU-4, use the **au-4tug-3**command in controller configuration mode.

au-4 *au-4-number* **tug-3** *tug-3-number*

Syntax Description

au-4-number	Number in the range from 1 to *x*where *x*is the STM level. Default is 1.
tug-3-number	Number in the range from 1 to 3.

Command Default

Default *au-4-number* value for the STM-1 card is 1.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
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.
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 **augmappingau-4**configuration controller command to map the AUG to a TUG-3 with the following muxing/alignment/mapping:

C-12 <--> VC-12 <--> TU-12< --> TUG-2 <--> TUG-3 <--> VC-4 <--> AU-4 <--> AUG

Configuring the **au-4**command enables you to enter configuration controller tug3 command mode and creates a serial interface with the following name format:

slot/port-adapter/port.au-4-number/tug-2-number/e1-number

The aug mapping au-4 and **au-4tug-3**commands are available only when SDH framing is configured.

Examples

The following example shows how to configure AUG mapping to be derived from a TUG-3 and selects TUG-3 1 of AU-4 1:

```
Router(config)# controller sonet 2/0/0
Router(config-controller)# aug mapping au-4
Router(config-ctrlr-tug3)# au-4 1 tug-3 1
```

Related Commands

Command	Description
au-3	Specifies an AU-3 for configuration.
aug mapping	Configures the AUG mapping mode.

aug mapping

To configure administrative unit group (AUG) mapping when Synchronous Digital Hierarchy (SDH) framing is selected, use the **augmapping** command in controller configuration mode.

aug mapping {**au-3** | **au-4**}

Syntax Description

au-3	Specifies use of three paths--a path is known as an Administrative Unit (AU)--consisting of seven Tributary Unit group type 2s (TUG-2s). Each TUG-2 consists of three virtual containers (VC-12s), which carry E1 lines resulting in 21 E1 lines within one AU-3 path.
au-4	Specifies use of one path consisting of three TUG-3 types. Each TUG-3 consists of seven TUG-2s, resulting in a total of 63 E1 lines within one AU-4 path. This is the default.

Command Default

au-4

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.0(17)S	Support for the two-port STM-1/OC-3 channelized E1/T1 line card was added.
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.
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series.

Usage Guidelines

In SDH, there are two possible mapping/multiplexing schemes for most payload types: ANSI and ETSI.

In ANSI mapping, the Low Order payloads are aggregated into a VC-3 High Order Path. An AU pointer is added to the VC-3 to create an AU-3. Three such AU-3s are then synchronously multiplexed into an AUG. The multiplexing scheme is as follows:

... VC-3 <-> AU-3 (x3) <-> AUG <-> STM-1

SDH ANSI mapping is very similar to the SONET frame structure.

In ETSI mapping, the Low Order payloads are aggregated into a VC-4 High Order Path. An AU pointer is added to the VC-4 to create an AU-4 (Administrative Unit type 4). One AU-4 is “multiplexed” into an AUG (AU group), which is to say, the AUG is, in fact, equivalent to an AU-4. The multiplexing scheme is as follows:

... TUG-3 (x3) <-> VC-4 <-> AU-4 (x1) <-> STM-1

This command is available only when SDH framing is configured.

This command does not have a **no** form because data must flow using one of the two mapping/multiplexing schemes.

Examples

The following example shows how to configure AU-3 mapping for the STM-1 trunk card:

```
Router(config)# controller sonet 1/0
Router(config-controller)# aug mapping au-3
```

aug mapping [au-3 | au-4] stm [stm number] stm1 number [number]

Use this command to configure mixed AU-3 and AU-4 mapping

aug mapping [*au-3* | *au-4*] **stm** [*stm number*] **stm1 number** [*number*].

Syntax Description

Syntax Description

au-3	Mode of augment mapping
au-4	Mode of augment mapping
stm	The STM-1 (Synchronous Transport Module level-1) is the SDH ITU-T fiber optic network transmission standard. It has a bit rate of 155.52 Mbit/s.
stm1 number	The STM number ranges from 1 to 4.

Command Default

The default mode is AU-4.

Command Modes

Global 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

The **aug mapping** command is available only when SDH framing is configured. AUG mapping is supported at STM-1 level.

Examples

```
enable
configure terminal
aug mapping [au-3 | au-4 stm [1-1] stm1 number [1-4]
end
```

Related Commands

Command	Description
show running configuration	Verifies aug mapping configuration.

aug mapping au-3 stm [stm number] path number [path number]

Use this command to change the AUG mapping of a particular STM-1 to AU-3.

aug mapping *au-3* **stm** [*1-16*] **path number** [*1-16*].

Syntax Description

Syntax Description

au-3	Mode of augment mapping
au-4	Mode of augment mapping
stm	The STM-1 (Synchronous Transport Module level-1) is the SDH ITU-T fiber optic network transmission standard. It has a bit rate of 155.52 Mbit/s.
path number	The path parameter number ranges from 1 to 16.

Command Default

The default mode is AU-4.

Command Modes

Global 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.

Examples

```
enable
configure terminal
aug mapping [au-3 | au-4 stm [1-16] path number [1-16]
end
```

Related Commands

Command	Description
show running configuration	Verifies aug mapping configuration.

auto-polarity

To enable automatic receiver polarity reversal on a hub port connected to an Ethernet interface of a Cisco 2505 or Cisco 2507 router, use the **auto-polarity** command in hub configuration mode. To disable this function, use the **no** form of this command.

auto-polarity
no auto-polarity

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Hub configuration

Command History

Release	Modification
10.3	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 applies to a port on an Ethernet hub only.

Examples

The following example shows how to enable automatic receiver polarity reversal on hub 0, ports 1 through 3:

```
Router(config)#
 hub ethernet 0 1 3
Router(config-hub)#
 auto-polarity
```

Related Commands

Command	Description
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

b2 sd-ber

To set the signal degrade bit-error rate (BER) threshold values, use the **b2sd-ber**command in controller configuration mode. To return to the default setting, use the **no** form of this command.

b2 sd-ber *rate*
no b2 sd-ber

Syntax Description

rate	Bit-error rate from 3 to 9 (10-n). The value of 9 represents better quality, and the value of 3 represents lower quality. The default is 6.

Command Default

rate: 6

Command Modes

Controller configuration

Command History

Release	Modification
12.2(15)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

Use this command to configure the threshold for degradation of quality of signal with b2 errors.

Examples

The following example shows how to configure a signal degrade BER threshold value of 7 on the SONET controller:

```
Router(config)# controller sonet 1/0
Router(config-controller)# b2 sd-ber 7
```

Related Commands

Command	Description
show controllers sonet	Displays information about the SONET controllers.

b2 sf-ber

To set the signal failure bit-error rate (BER) threshold values, use the **b2sf-ber**command in controller configuration mode. To return to the default setting, use the **no** form of this command.

b2 sf-ber *rate*
no b2 sf-ber *rate*

Syntax Description

rate	Bit-error rate from 3 to 9 (10-n). The value of 9 represents better quality, and the value of 3 represents lower quality. The default is 3.

Command Default

rate : 3

Command Modes

Controller configuration

Command History

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

Usage Guidelines

Use this command to configure the threshold for failure of quality of signal with b2 errors. The value of 9 represents better quality and the value of 3 represents lower quality.

Examples

The following example shows how to configure a signal failure BER threshold value of 7 on the SONET controller:

```
Router(config)# controller sonet 1/0
Router(config-controller)# b2 sf-ber 7
```

Related Commands

Command	Description
show controllers sonet	Displays information about the SONET controllers.

backup delay

To define how much time should elapse before a secondary line status changes after a primary line status has changed, use the **backupdelay**command in interface configuration mode. To return to the default so that as soon as the primary fails, the secondary is immediately brought up without delay, use the **no** form of this command.

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

Syntax Description

enable-delay-period	Number of seconds that elapse after the primary line goes down before the Cisco IOS software activates the secondary line.
disable-delay-period	Number of seconds that elapse after the primary line comes up before the Cisco IOS software deactivates the secondary line.
never	Secondary line is never activated or deactivated.

Command Default

0 second delay

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

For environments in which spurious signal disruptions appear as intermittent lost carrier signals, we recommend that you enable some delay before activating and deactivating a secondary line.

For the Cisco 7600 Backup Interface for Flexible UNI feature to work correctly, the enable and disable backup delay must be 0.

Examples

The following example sets a 10-second delay on deactivating the secondary line (serial interface 0); however, the line is activated immediately.

```
interface serial 0
 backup delay 0 10
```

backup interface

To configure an interface as a secondary or a dial backup, use the **backupinterface**command in interface configuration mode. To disable the interface from serving as a backup, use the **no** form of this command.

Cisco 7200 Series and Cisco 7600 Series Routers Only
backup interface *slot/port-adapter/port*
no backup interface *slot/port-adapter/port*

Other Cisco Routers
backup interface *type number*
no backup interface *type number*

Syntax Description

slot / port-adapter / port	Chassis slot, port adapter, and port number of the interface to configure as a backup. Include a slash (/) between the slot, port adapter, and port (for example, 1/1/1). See your hardware installation manual for the specific slot, port adapter, and port numbers.
type number	Type and port number of the interface that is being configured as a backup.

Command Default

An interface is not configured as a backup.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

The interface that you define with the **backupinterface** command can back up only one interface.

Serial, ISDN, and Ethernet backup interfaces are supported by the routers. Access servers support both asynchronous backup interfaces and serial backup interfaces.

In Cisco IOS Release 12.2(33)SRB1 and later releases, you can configure a backup interface for Gigabit Ethernet interface on the Cisco 7600 router. The backup interface works only when the configurations on the primary and backup interfaces are identical. This is applicable to all Cisco IOS platforms and interfaces.



Note If the interface configuration includes the **xconnect**command, you must specify a different virtual circuit ID (VCID) on the primary and backup interfaces.

Examples

The following example sets serial interface 1 as the backup line to serial interface 0:

```
Router(config)# interface serial 0
Router(config-if)# backup interface serial 1
```

The following example sets Gigabit Ethernet interface 4/0/1 as the backup interface for Gigabit Ethernet interface 3/0/1 on the Cisco 7600 router:

```
Router(config)# interface gigabitEthernet 3/0/1
Router(config-if)# backup interface gigabitEthernet 4/0/1
```

Related Commands

Command	Description
aps protect (SONET)	Enables SONET APS.
show version	Displays information about the currently loaded software along with hardware and device information.

backup interface atm

To back up a locally switched ATM connection, use the **backupinterfaceatm**command in **theconnectsub**mode. To deconfigure the active routing policy set, leaving the SBE with no active routing policy set, use the **no** form of this command.

backup interface atm *x/y/z vpi/vci*
no backup interface atm *x/y/z vpi/vci*

Syntax Description

interface	Identifies the interface.
atm > *x* / *y* / *z* >	Specifies the backup location for the ATM slot/subslot/port to be backed up.
vpi / *vci* >	Specifies the backup location for the ATM virtual path identifier/virtual channel identifier (VPI/VCI).

Command Default

No default behavior or values.

Command Modes

Connect submode (config-connection)

Command History

Release	Modification
12.2(33)SRC	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

- Only the tail end AC can be backed up; if head end fails there is no protection.
- The circuit type of the primary and backup AC must be identical (failover operation will not switch between different types of interfaces).
- Autoconfiguration is allowed for backup ATM Permanent Virtual Circuits (PVCs) or ATM Permanent Virtual Paths (PVPs).
- Dynamic modification of parameters in a local switching connection is not supported in the case where the tail-end segment is backed up to a segment using the **backupinterfaceatm**command. If you want to modify the parameters in any of the three segments (head-end, tail-end, or backup segment), you must first unconfigure with the **backupinterfaceatm** command, make the changes in the individual segments, and then reconfigure the backup with the **backupinterfaceatm** command.

Examples

The following is an example of a ATM virtual path local switching backup:

```
Router(config)# connect ATM atm2/0/0 0 atm3/0/0 0
Router(config-connection)# backup interface atm 4/0/0 1
```

The following is an example of a ATM virtual channel local switching backup:

```
Router(config)# connect ATM atm2/0/0 24/56 atm3/0/0 24/57
Router(config-connection)# backup interface atm 4/0/0 25/58
!
```

Related Commands

Command	Description
connect atm	Configures a local switching connection.

backup interface cem

To back up a locally switched CEM connection, use the **backupinterfacecem** command in **theconnectsub**mode. To deconfigure the locally switched CEM connection backup, use the **no** form of this command.

backup interface cem *x/y/z cemckt*
no backup interface cem *x/y/z cemckt*

Syntax Description

interface >	Identifies the interface.
cem > *x / y / z*	Specifies the CEM interface slot, subslot, and port to be backed up.
cemckt	Specifies the backup location for the CEM.

Command Default

No default behavior or values.

Command Modes

Connect submode (config-connection)

Command History

Release	Modification
12.2(33)SRC	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

- Autoconfiguration of CEM interfaces is not supported.
- Only the tail end AC can be backed up; if head end fails there is no protection.
- The circuit type of the primary and backup AC must be identical (failover operation will not switch between different types of interfaces or different CEM circuit types).
- Backs up a local switching connection to cem-ckt3 of CEM interface cem3. Only one backup AC is allowed for each connection.
- Autoconfiguration of backup CEM circuits is not allowed.
- The CEM circuit used as a backup in a local switching connection cannot be used for xconnect configurations.
- Dynamic modification of parameters in a local switching connection is not supported in the case where the tail-end segment is backed up to a segment using the **backupinterfacecem**command. If you want to modify the parameters in any of the three segments (head-end, tail-end, or backup segment), you must first unconfigure with the **backupinterfacecem**command, make the changes in the individual segments, and then reconfigure the backup with the **backupinterfacecem** command.

Examples

The following is an example of a CEM local switching backup:

```
Router(config)# connect cema cem4/3/0 0 cem2/0/0 0
Router(config-connection)# backup interface cem 2/0/0 1
```

Related Commands

Command	Description
connect cem	Configures a local switching connection.

backup load

To set a traffic load threshold for dial backup service, use the **backuploadcommand** in interface configuration mode. To return to the default value, use the **no** form of this command.

backup load {*enable-threshold* | **never**} {*disable-load* | **never**}
no backup load {*enable-threshold* | **never**} {*disable-load* | **never**}

Syntax Description

enable-threshold	Percentage of the primary line's available bandwidth that the traffic load must exceed to enable dial backup.
disable-load	Percentage of the available bandwidth that the traffic load must be less than to disable dial backup. The transmitted or received load on the primary line plus the transmitted or received load on the secondary line is less than the value entered for the *disable-load*argument to disable dial backup.
never	The secondary line is never activated or deactivated because of the traffic load.

Command Default

No threshold is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.

Usage Guidelines

When the transmitted or received load on the primary line is greater than the value assigned to the *enable-threshold* argument, the secondary line is enabled.

The secondary line is disabled when one of the following conditions occurs:

- The transmitted load on the primary line plus the transmitted load on the secondary line is less than the value entered for the *disable-load*argument.
- The received load on the primary line plus the received load on the secondary line is less than the value entered for the *disable-load* argument.

If the **never**keyword is used instead of an *enable-threshold*argument, the secondary line is never activated because of traffic load. If the **never** keyword is used instead of a *disable-load* argument, the secondary line is never activated because of traffic load.

Examples

The following example sets the traffic load threshold to 60 percent of the primary line serial 0. When that load is exceeded, the secondary line is activated and will not be deactivated until the combined load is less than 5 percent of the primary bandwidth.

```
interface serial 0
 backup load 60 5
 backup interface serial 1
```

bandwidth (interface configuration)

To set the inherited and received bandwidth values for an interface, use the **bandwidth** command in interface or virtual network interface config mode. To restore the default values, use the **no** form of this command.

bandwidth [**receive**] {*kbps* | **inherit** [*kbps*]}
no bandwidth [**receive**] {*kbps* | **inherit** [*kbps*]}

Syntax Description

kbps	Intended bandwidth, in kilobits per second. The range is from 1 to 10000000. For a full bandwidth DS3 line, enter the value 44736.
inherit	(Optional) Specifies how a subinterface inherits the bandwidth of its main interface.
receive	(Optional) Enables asymmetric transmit/receive operations so that the transmitted (**inherit** *kbps*) and received bandwidth are different.

Command Default

Default bandwidth values are set during startup. The bandwidth values can be displayed using the **show interfaces** or **show ipv6 interface** command. If the **receive** keyword is not used, by default, the transmit and receive bandwidths will be assigned the same value.

Command Modes

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.2T	This command was modified. The **inherit** keyword was added.
12.4(6)T	This command was modified. Support for IPv6 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.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 Aggregation Services Series Routers.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.
15.1(03)S	This command was modified. Support was added for the **receive** keyword.

Usage Guidelines

Bandwidth Information

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

Note This is only a routing parameter. It does not affect the physical interface.

Changing Bandwidth

For some media, such as Ethernet, the bandwidth is fixed; for other media, such as serial lines, you can change the actual bandwidth by adjusting the hardware. For both classes of media, you can use the **bandwidth** command to communicate the current bandwidth to the higher-level protocols.

Bandwidth Inheritance

Before the introduction of the **bandwidth inherit** command option, when the bandwidth value was changed on the main interface, the existing subinterfaces did not inherit the bandwidth value. If the subinterface was created before the bandwidth was changed on the main interface, the subinterface would receive the default bandwidth of the main interface, and not the configured bandwidth. Additionally, if the router was subsequently reloaded, the bandwidth of the subinterface would then change to the bandwidth configured on the main interface.

The **bandwidth inherit** command controls how a subinterface inherits the bandwidth of its main interface. This functionality eliminates inconsistencies related to whether the router has been reloaded and what the order was in entering the commands.

The **no bandwidth inherit** command enables all subinterfaces to inherit the default bandwidth of the main interface, regardless of the configured bandwidth. If the **bandwidth inherit** command is used without configuring a bandwidth on a subinterface, all subinterfaces will inherit the current bandwidth of the main interface. If you configure a new bandwidth on the main interface, all subinterfaces will use this new value.

If you do not configure a bandwidth on the subinterface and you configure the **bandwidth inherit** *kbps* command on the main interface, the subinterfaces will inherit the specified bandwidth.

In all cases, if an explicit bandwidth setting is configured on an interface, the interface will use that setting, regardless of whether the bandwidth inheritance setting is in effect.

Bandwidth Receipt

Some interfaces (such as Asymmetric Digital Subscriber Line (ADSL), V.35, RS-449, and High-Speed Serial Interface (HSSI)) can operate with different transmit and receive bandwidths. The **bandwidth receive** command permits this type of asymmetric operation. For example, for ADSL, the lower layer detects the two bandwidth values and configures the Integrated Data Base (IDB) accordingly. Other interface drivers, particularly serial interface cards on low- and midrange-platforms, can operate in this asymmetric bandwidth mode but cannot measure their clock rates. In these cases, administrative configuration is necessary for asymmetric operations.

Examples

The following example shows how to set the full bandwidth for DS3 transmissions:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth 44736
```

The following example shows how to set the receive bandwidth:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth receive 1000
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.
show ipv6 interface	Displays statistics for all interfaces configured on the IPv6 router.

batch

To allow better cache utilization at the interface level, use the batch command under interface configuration mode.

batch {allowed | **count***number* | **threshold***range* **}**

Syntax Description

allowed	Enables the batch process for packets received.
count *number*	Number of interrupts received for the batch process. Value ranges from 2 to 8. When batching is enabled, the packets in the receive ring are processed on every nth RX interrupt, where "n" is configured by "batch count n".
threshold *range*	Packets per 4ms threshold to enable the batch. Range is from 2 to 100 packets/4ms. If the number of packets received within a 4ms period exceeds 'x' then batching is turned on, otherwise it is turned off.

Command Default

Batch is disabled.

Command Modes

configuration-Interface

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use this command to increase the performance of packets processing through the interface to optimize the cache usage. The performance improvement varies depending on the burstiness of the traffic. The traffic with high burstiness provides better performance.

The **batch** command is disabled by default. The batch process depends on the batch threshold (x) which is the number of packets received within a ‘y’ ms period. The batch process is turned on if the number of packets received within a ‘y’ ms period exceeds ‘x’, otherwise it is turned off.

Currently, the batch command is supported at the interface level on Cisco 890 routers only.

Examples

The following example shows the batch command configured in interface fastethernet ports:

```
        !
!
interface FastEthernet0
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet1
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
```

```
interface FastEthernet2
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet3
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet4
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet5
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet6
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
interface FastEthernet7
 no ip address
 batch allowed
 batch count 6
 batch threshold 75
!
!
```

bert abort controller

To end a bit error rate testing (BERT) session, use the **bertabortcontroller**command in privileged EXEC mode.

bert abort controller *controller-type slot/port*

Syntax Description

controller-type	Type of controller being tested. Use either T1 or E1 depending on the type of facility.
slot / port	Slot number and port number to end a BERT session.

Command Default

A BERT session is configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)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

Use the **bertabortcontroller**command to cancel bit error rate testing on each port of the Cisco AS5300 router.

The BERT feature enables you to test the quality of the connected Primary Rate Interface (PRI) links by direct comparison of a pseudorandom or repetitive test pattern with an identical locally generated test pattern.

Examples

The following is sample output from the **bertabortcontroller**command when no bit error rate test is running:

```
Router# bert abort controller t1 0/0
Router#
17:53:33: There is no BERT Test running ....
```

The following is sample output from the **bertabortcontroller**command when a bit error rate test is running:

```
Router# bert abort controller t1 0/0
Do you really want to abort the current BERT [confirm] Y17:56:56: %BERT-6-BERT_RESULTS:
Controller T1 0 Profile default : The Test was
aborted by User
```

Related Commands

Command	Description
bert controller	Starts a bit error rate test for a particular port.

Command	Description
bert pattern (**T1/E1**)	Sets up various bit error rate testing profiles.

bert controller

To start a bit error rate test (BERT) for a particular port, use the **bertcontroller**command in privileged EXEC mode.

bert controller *controller-type controller-number last-controller-number* **profile** {*profile-number* [*last-profile-number*] [**timeslot** *timeslot-number* [*last-timeslot-number*]] | **default**}

Syntax for Cisco 2600 Platforms
bert controller *type-controller slot/port* [**channel-group** *channel-number*] [**pattern** *pattern-name*] [**interval** *range*]

Syntax Description

controller-type	Type of controller being tested. Use either T1 or E1 depending on the type of facility.
controller-number	Controller number. The valid range is from 0 to 7.
last-controller-number	Last contoller number. The valid range is from 2 to 7.
profile	Sets the profile numbers for the bit error rate test.
profile-number	Numbers of the test profiles to use. The valid range is from 0 to 15. The default is 0.
last-profile-number	(Optional) Last profile number. The default is 0.
timeslot	(Optional) Generates the data based on the timeslots associated with the controller.
timeslot-number	(Optional) Timeslot number. The valid range is from 1 to 22.
last-timeslot-number	(Optional) Last timeslot number. The valid range is from 1 to 24.
default	Executes the default bit error rate test (0).
slot/port	Slot and port number for the ports to be tested.
channel-group *channel-number*	(Optional) Specifies the channel group number that you want the BERT test to run on. Numbers can be 0 or 1.

pattern *pattern-name*	(Optional) BERT patterns available for testing are: • 0s--repetitive pattern; all zeros test pattern • 1s--n repetitive pattern; all ones test pattern • qrw--215-1 QRW test pattern • qrss (default)--220-1 Quasi-Random Signal Sample 0.151 test pattern • alt-0-1--alternating zeros and ones test pattern • 1in8--n repetitive pattern; 1 in 8 • 3in24--n repetitive pattern; 3 in 24 • 63--26-1 63 test pattern • 511--29-1 511 test pattern • 2047--211-1 test pattern
interval *range*	(Optional) Range for the test, in minutes. The valid range is from 1 to 14400. The default is 1.

Command Default

The test profile 0 is configured by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(2)XD	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)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.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The following keywords and arguments were added: • *last-controller-number* • *last-profile-number* • **timeslot** • *timeslot-number* • *last-timeslot-number* • **default**

Usage Guidelines

Use the **bertcontroller** command to start a bit error rate test for a particular port on a Cisco AS5300 router.

Quality Testing

The BERT feature enables you to test the quality of the connected Primary Rate Interface (PRI) links by direct comparison of a pseudorandom or repetitive test pattern with an identical locally generated test pattern.

E1 Controllers

The E1 controller cannot be set in loopback mode from the Cisco AS5300 router. For the **bertcontroller** command to work correctly with the E1 controller, the controller must be configured as a channel group or as channel-associated signaling (CAS) and the line must be configured as a remote loop from the switch side of the link.

You can use the **channel-group***channel-group-number* keyword and argument combination to specify a channel-group. If the channel-group is specified, BERT will be run on the timeslots associated with the channel group only. Otherwise, BERT will run on all the timeslots of the specified controller.

Examples

The following is sample output from the **bertcontroller** command:

```
Router#
bert controller T1 T2 profile default
Press <Return> to start the BERT [confirm]
Y
17:55:34: %BERT-6-BERT_START: Starting BERT on Interface 0 with Profile default
Data in current interval (10 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Table 1 describes the significant fields shown in the display.

*Table 1: **bert controller** Field Descriptions*

Field	Description
Data in current interval	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. As the latest 15-minute accumulation period enters the buffer, the oldest 15-minute period is deleted. The accumulation period is from 1 to 900 seconds.
Line Code Violations	For alternate mark inversion (AMI)-coded signals, a line code violation is a bipolar violation (BPV) occurrence. Indicates the occurrence of either a BPV or an excessive zeros (EXZ) error event.
Path Code Violations	When super frame (SF) (D4) framing is used, a path code violation is a framing error. When extended super frame (ESF) framing is used, a path code violation is a cyclic redundancy check type 6 (CRC-6) error. Indicates a frame-synchronization bit error in the D4 and E1-non-CRC formats, or a CRC error in the ESF and E1-CRC formats.
Slip Secs	Indicates the replication or deletion of the payload bits of a DS1 frame. A slip may be indicated when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Seconds during which the framing pattern has been lost. Indicates the number of seconds for which an Out-of-Frame error is detected.

Field	Description
Line Err Secs	A line error second (LES) is a second in which one or more line code violation (LCV or CV-L) errors are detected.
Degraded Mins	A degraded minute is one in which the estimated error rate exceeds 1-6 but does not exceed 1-3.
Errored Secs	In extended superframe (ESF) and E1-CRC links, an errored second is a second in which one of the following is detected: one or more path code violations; one or more Out-of-Frame defects; one or more controlled slip events; an alarm indication signal (AIS) defect. For D4 and E1-non-CRC links, the presence of bipolar violations also triggers an errored second.
Bursty Err Secs	Seconds with fewer than 320 and more than 1 path code violation error, no severely errored frame defects, and no detected incoming AIS defects. Controlled slips are not included in this parameter.
Severely Err Secs	For ESF signals, a second with one of the following errors: 320 or more path code violation errors; one or more Out-of-Frame defects; a detected AIS defect. For E1-CRC signals, a second with one of the following errors: 832 or more path code violation errors; one or more Out-of-Frame defects. For E1-non-CRC signals, a second with 2048 or more line code violations. For D4 signals, a count of 1-second intervals with framing errors, or an Out-of-Frame defect, or 1544 line code violations.
Unavail Secs	Count for every second in which an unavailable signal state occurs. This term is used by new standards in place of failed seconds (FS).

The following example shows a BERT test started on a T1 port 0/0 and channel group 0 with a QRSS signaling pattern for a duration of 5 minutes:

```
Router# bert controller t1 0/0 channel-group 0 pattern qrss interval 5
```

Related Commands

Command	Description
bert abort	Aborts a bit error rate testing session.
bert pattern (T1/E1)	Sets up various bit error rate testing profiles.
bert abort controller	Stops a BERT test prematurely.

bert errors

To transmit bit error ratio test (BERT) errors while running any BERT pattern, use the**berterror**command in interface configuration mode.

bert errors [*number*]

Syntax Description

number	(Optional) Range of **1-255**BERT errors that may be introduced in a BERT pattern.

Command Default

Default is 1.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(12c)EX1	This command was introduced for Cisco 7304 routers.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series router and Catalyst 6500 series switch.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to test link availability by injecting a fixed number of bert errors when a pattern is running and check that the same number of errors were received on the remote end.

Examples

This example injects 200 BERT errors in a running bit pattern on slot 5, subslot 0.

```
Router# configure terminal
Router(config)# interface serial 5/0/0
Router(config-if)# bert errors 200
```

Related Commands

Command	Description
bert pattern	Starts a BERT pattern on a port.
show controller serial	Displays serial line statistics.

bert pattern

To start a BERT pattern on a port, use the **bertpattern**command in interface configuration mode. Use the no bert pattern command to stop the sequence.

bert pattern {**0s** | **1s** | **2^11** | **2^15** | **2^20** | **2^23** | **alt-0-1** | **qrss**} **interval** *minutes*
no bert pattern {**0s** | **1s** | **2^11** | **2^15** | **2^20** | **2^23** | **alt-0-1** | **qrss**} **interval** *minutes*

Syntax Description

0s	Repeating pattern of zeros (...000...).
1s	Repeating pattern of ones (...111...).
2^11	Pseudo-random repeating test pattern that consists of 2,048 bits.
2^15	Pseudorandom 0.151 test pattern that is 32,768 bits in length.
2^20	Pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
2^23	Pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
alt-0-1	Repeating pattern of alternating zeros and ones (...01010...).
qrss	Pseudorandom quasi-random signal sequence (QRSS) 0.151 test pattern that is 1,048,575 bits in length.
interval *minutes*	Specifies the length of the BERT test in minutes.

Command Default

Bert is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	The command was introduced.
12.0(5)XE	The command was enhanced as an ATM interface configuration command
12.0(7)XE1	Support for Cisco 7100 series routers was added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(12c)EX1	Support for Cisco 7304 routers was added.
12.2(18)S	Support for Cisco 7304 routers was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on the Cisco 7600 series router and the Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
XE3.18SP	This command was integrated into Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.

Usage Guidelines

Use the bert pattern commamd to start or stop a specific bit pattern. To test link availability, start a pattern on one end and put the remote end in network loopback and verify that there are no bert errors.

Examples

This example starts a bert pattern on slot 5, bay 0.

```
Router# configure terminal
Router(config)# int serial 5/0/0
Router(config-if)# bert pattern 0s
```

This example starts a bert pattern pRBS.

```
Router#enable
Router#configure terminal
Router(config)#bert pattern pRBS interval 5 direction line
exit
```

Related Commands

Command	Description
bert errors	Transmit bert errors while running any bert pattern.
loopback	Loopback at various points in the transmit and receive path.
show controller serial	Displays serial line statistics.
show controller sonet	Displays sonet interface module statistics.
show controller t1	Displays t1 interface module statistics.
show controller t3	Displays t3 interface module statistics.

bert pattern (T1 E1)

To enable a bit error rate test (BERT) pattern on a T1 or E1 line, use the**bertpattern**command in controller configuration mode. To disable a BER test pattern, use the **no** form of this command.

bert pattern *pattern* **interval** *time*
no bert pattern *pattern* **interval** *time*

Syntax Description

pattern	The test pattern indicated by any of the following allowable values:
2^23	Invokes a pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
2^20	Invokes a pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
2^20-QRSS	Invokes a pseudorandom quasi-random signal sequence (QRSS) 0.153 test pattern that is 1,048,575 bits in length.
2^15	Invokes a pseudorandom 0.151 test pattern that is 32,768 bits in length.
2^11	Invokes a pseudorandom test pattern that is 2,048 bits in length.
1s	Invokes a repeating pattern of ones (...111...).
0s	Invokes a repeating pattern of zeros (...000...).
alt-0-1	Invokes a repeating pattern of alternating zeros and ones (...01010...).
interval *time*	Specifies the duration (in minutes) of the BER test. The interval can be a value from 1 to 14400. There is no default.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)XE	This command was enhanced as an ATM interface configuration command.
12.0(7)XE1	This command was implemented on 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

BER testing is supported on each of the T1 or E1 lines, is done only over an unframed T1 or E1 signal, and is run on only one port at a time.

To view the BER test results, use the **showcontrollersatm**EXEC command. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BER test
- Total bit errors
- Total bits received

When the T1 or E1 line has a BER test running, the line state is DOWN and the status field shows the current/last result of the test.

The**bertpattern**command is not written to NVRAM because this command is only used to test the T1 or E1 line for a short predefined interval, and to avoid accidentally saving the command.

Examples

The following example shows how to run a BERT pattern of all zeros on a Cisco 7200 series router for 30 minutes on the T1 controller in slot 1:

```
Router(config)#
controller T1 1/0
Router(config-if)#
bert pattern 0s interval 30
```

Related Commands

Command	Description
show controllers atm	Displays information about T1/E1 links in Cisco 7100 series routers, Cisco 7200 series routers, and Cisco 7500 series routers.

bert pattern (T3 E3)

To enable a bit error rate test (BERT) pattern on a T3 or E3 controller, use the **bertpattern** command in controller configuration mode. To disable a BER test pattern, use the no form of this command.

bert pattern *pattern* **interval** *time*
no bert pattern

Syntax Description

pattern	The pattern indicated by any of the following allowable values:
2^23	Invokes a pseudorandom 0.151 test pattern that is 8,388,607 bits in length.
2^20	Invokes a pseudorandom 0.153 test pattern that is 1,048,575 bits in length.
2^15	Invokes a pseudorandom 0.151 test pattern that is 32,768 bits in length.
1s	Invokes a repeating pattern of ones (...111...).
0s	Invokes a repeating pattern of zeros (...000...).
alt-0-1	Invokes a repeating pattern of alternating zeros and ones (...01010...).
interval *time*	Specifies the duration (in minutes) of the BER test. The interval can be a value from 1 to 14400. There is no default.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
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(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

BER testing is supported on T3/E3 links and is done only over framed T3 or E3 signals, unless E3 framing is in bypass mode.

To display the BER test results, use the show controllers t3 or show controllers e3 EXEC command. The BER test results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BER test
- Total bit errors
- Total bits received

When the T3 or E3 line has a BER test running, the line state is DOWN and the status field shows the current or last result of the test.

The**bertpattern**command is not written to NVRAM because this command is used only to test the T3 or E3 line for a short predefined interval, and to avoid accidentally saving the command.

Examples

The following example shows how to run a BERT pattern of all zeros for 30 minutes on the T3 controller in slot 1:

```
Router(config)#
controller T3 1/0
Router(config-if)#
bert pattern 0s interval 30
```

Related Commands

Command	Description
show controllers e3	Displays information about E3 controllers.
show controllers t3	Displays information about T3 controllers.

bert profile

To set up various bit error rate testing profiles, use the **bert profile** command in global configuration mode. To disable the particular bit error rate test (BERT) profile indicated by profile number, use the **no** form of this command.

bert profile *number* **pattern** *pattern* **threshold** *threshold* **error-injection** *err-inj* **duration** *time*
no bert profile *number* **pattern** *pattern* **threshold** *threshold* **error-injection** *err-inj* **duration** *time*

Syntax Description

number	BERT profile number. The valid range is from 1 to 15. This is the number assigned to a particular set of parameters. If no such profile of the same number exists in the system, a new profile is created with that number; otherwise, an existing set of parameters with that profile number is overwritten by the new profile.
pattern	Pattern that BERT will generate on the line.
pattern	**0s** --Repetitive pattern, all zeros.**1_in_16**--n repetitive pattern, 1 in 16.**1s**--n repetitive pattern, all ones.**211-O.152**--n pseudorandom pattern, 211 -1 O.152.**215-O.15**--n pseudorandom pattern, 215 -1 O.151.**220-O.151QRSS**--n pseudorandom pattern, 220 -1 O.151 QRSS. (This is the default.)**220-O.153**--n pseudorandom pattern, 220 -1 O.153.**3_in_24**--n repetitive pattern, 3 in 24.
threshold	Test failure (error) threshold that determines if the BERT on this line passed.
threshold	**10^-2** --Bit error rate of 10-2.**10^-3**--Bit error rate of 10-3.**10^-4**--Bit error rate of 10-4.**10^-5**--Bit error rate of 10-5.**10^-6**--Bit error rate of 10-6. (This is the default.)**10^-7**--Bit error rate of 10-7.**10^-8**--Bit error rate of 10-8.
error-injection	Error injection rate for bit errors injected into the BERT pattern generated by the chip.
err-inj	**10^-1** --Error injection of 10-1.**10^-2**--Error injection of 10-2.**10^-3**--Error injection of 10-3.**10^-4**--Error injection of 10-4.**10^-5**--Error injection of 10-5.**10^-6**--Error injection of 10-6.**10^-7**--Error injection of 10-7.**none**--No error injection in the data pattern. (This is the default.)
duration	Duration, in minutes, for which BERT is to be executed.
time	Duration of BERT, in minutes. The valid range is from 1 to 1440. The default is 10.

Command Default

The default profile created internally by the system has parameters that cannot be changed. This profile has been defined so that you can execute BERT on a line without having to configure a new profile. The default profile is displayed when the running configuration is displayed and is not stored in NVRAM:

bert profile *number* **pattern 220-0151QRSS threshold 10^-6 error-injection none duration 10**

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)XD	This command was introduced.

Release	Modification
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)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

Use the **bert profile** command to set up bit error rate testing profiles for the Cisco AS5300 router.

The bit error rate test (BERT) feature enables you to test the quality of the connected PRI links by direct comparison of a pseudorandom or repetitive test pattern with an identical locally generated test pattern. A BERT profile is a set of parameters related to a BERT test and is stored as part of the configuration in NVRAM. You can define up to 15 BERT profiles on the system. By setting up the BERT profiles in this way, you do not have to enter the parameters each time you want to run a BERT--just select the number of the BERT profile that you want to run.

Examples

The following example shows a configured BERT profile number 1 to have a 0s test pattern, with a 10-2 threshold, no error injection, and a duration of 125 minutes:

```
Router(config)#
bert profile 1 pattern 0s threshold 10^-2 error-injection none duration 125
```

Related Commands

Command	Description
bert abort	Aborts a bit error rate testing session.
bert controller	Starts a bit error rate test for a particular port.

bitswap line

To divert the data of a disturbed transmission channel to other channels, use the **bitswap line** command in controller configuration mode. To disable bitswapping, use the **no** form of this command.

bitswap [line *line-number***]**
no bitswap [line *line-number***]**

Syntax Description

line-number	Line number. Valid values are either 0 or 1.

Command Default

Bit swapping is enabled.

Command Modes

Controller configuration (config-controller)#

Command History

Release	Modification
15.4(4)T	This command was introduced.

Usage Guidelines

- After you enable bit swapping, whenever the line conditions change, the modem swaps the bits around different channels without retraining.
- If you enable bonded mode, bit swapping will be enabled on both the lines.
- If you specify only the line number, bit swapping will be enabled only on that line.
- In case of single mode, bit swapping will be enabled only on that line.

Examples

The following example shows how to enable bit swapping on line 0:

```
Router(config-controller)# bitswap line 0
```

The following example shows how to disable bit swapping:

```
Router(config-controller)# no bitswap
```

Related Commands

Command	Description
sra line	Accommodates changes to the total link capacity with less disruption to communications.

bridge-domain

To enable RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI), use the **bridge-domain**command in Frame Relay DLCI configuration, interface configuration, interface ATM VC configuration, or PVC range configuration mode. To disable bridging, use the **no** form of this command.

bridge-domain *vlan-id* [**access** | **dot1q** [*tag*] | **dot1q-tunnel**] [**broadcast**] [**ignore-bpdu-pid**] [**pvst-tlv** *CE-vlan*] [**increment**] [**lan-fcs**] [**split-horizon**]
no bridge-domain *vlan-id*

Syntax Description

vlan-id	The number of the VLAN to be used in this bridging configuration. The valid range is from 2 to 4094.
access	(Optional) Enables bridging access mode, in which the bridged connection does not transmit or act upon bridge protocol data unit (BPDU) packets.
dot1q	(Optional) Enables Institute of Electrical and Electronic Engineers (IEEE) 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. If this keyword is not specified, the ingress side assumes a CoS value of 0 for quality of service (QoS) purposes.
tag	(Optional--ATM PVCs only) Specifies the 802.1Q value in the range 1 to 4095. You can specify up to 32 **bridge-domain** command entries using **dot1q***tag* for a single PVC. The highest tag value in a group of **bridge-domain** commands must be greater than the first tag entered (but no more than 32 greater).
dot1q-tunnel	(Optional) Enables IEEE 802.1Q tunneling mode, so that service providers can use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs.
broadcast	(Optional) Enables bridging broadcast mode on this PVC. This option is not supported for multipoint bridging. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
ignore-bpdu-pid	(Optional for ATM interfaces only) Ignores BPDU protocol identifiers (PIDs) and treats all BPDU packets as data packets to allow interoperation with ATM customer premises equipment (CPE) devices that do not distinguish BPDU packets from data packets.
pvst-tlv	(Optional) When the router or switch is transmitting, translates Per-VLAN Spanning Tree Plus (PVST+) BPDUs into IEEE BPDUs. When the router or switch is receiving, translates IEEE BPDUs into PVST+ BPDUs.
CE-vlan	Customer-edge VLAN in the Shared Spanning Tree Protocol (SSTP) tag-length-value (TLV) to be inserted in an IEEE BPDU to a PVST+ BPDU conversion.
increment	(PVC range configuration mode only) (Optional) Increments the bridge domain number for each PVC in the range.

lan-fcs	(Optional) Specifies that the VLAN bridging should preserve the Ethernet LAN frame checksum (FCS) of the Ethernet frames across the ATM network. **Note** This option applies only to routers using a FlexWAN module. Support for this option was removed in Cisco IOS Release 12.2(18)SXF2 and Cisco IOS Release 12.2(33)SRA.
split-horizon	(Optional) Enables RFC 1483 split horizon mode to globally prevent bridging between PVCs in the same VLAN.

Command Default

Bridging is disabled.

Command Modes

Frame Relay DLCI configuration (config-fr-dlci) Interface configuration (config-if)--Only the **dot1q** and **dot1q-tunnel** keywords are supported in interface configuration mode. Interface ATM VC configuration (config-if-atm-vc) PVC range configuration (config-if-atm-range)

Command History

Release	Modification
12.1(13)E	This command was introduced as the **bridge-vlan** command for the 2-port OC-12 ATM WAN Optical Services Modules (OSMs) on Cisco 7600 series routers and Catalyst 6500 series switches.
12.1(12c)E	This command was integrated into Cisco IOS Release 12.1(12c)E.
12.1(14)E1	This command was integrated into Cisco IOS Release 12.1(14)E1. The **dot1q-tunnel** keyword was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **dot1q-tunnel** keyword is not supported in this release.
12.1(19)E	The **split-horizon** keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The **dot1q-tunnel** and **split-horizon** keywords are supported in this release.
12.2(17a)SX	Support was added for the **dot1q-tunnel** keyword in Cisco IOS Release 12.2(17a)SX.
12.2(18)SXE	This command was renamed from **bridge-vlan** to **bridge-domain**. The **access**, **broadcast**, **ignore-bpdu-pid**, and **increment** keywords were added.
12.2(18)SXF2	Support for the **lan-fcs** and **broadcast**keywords was removed. The **ignore-bpdu-pid**and **pvst-tlv**keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

RFC 1483 bridging on ATM interfaces supports the point-to-point bridging of Layer 2 packet data units (PDUs) over Ethernet networks. RFC 1490 Frame Relay bridging on Packet over SONET (POS) or serial interfaces that are configured for Frame Relay encapsulation provides bridging of Frame Relay packets over Ethernet networks.

The Cisco 7600 router can transmit BPDUs with a PID of either 0x00-0E or 0x00-07. When the router connects to a device that is fully compliant with RFC 1483 Appendix B, in which the IEEE BPDUs are sent and received by the other device using a PID of 0x00-0E, you must not use the **ignore-bpdu-pid**keyword.

If you do not enter the **ignore-bpdu-pid** keyword, the PVC between the devices operates in compliance with RFC 1483 Appendix B. This is referred to as *strict mode* . Entering the **ignore-bpdu-pid** keyword creates *loose mode* . Both modes are described as follows:

- Without the **ignore-bpdu-pid**keyword, in strict mode, IEEE BPDUs are sent out using a PID of 0x00-0E, which complies with RFC 1483.
- With the **ignore-bpdu-pid**keyword, in loose mode, IEEE BPDUs are sent out using a PID of 0x00-07, which is normally reserved for RFC 1483 data.

Cisco-proprietary PVST+ BPDUs are always sent out on data frames using a PID of 0x00-07, regardless of whether you enter the **ignore-bpdu-pid** keyword.

Use the **ignore-bpdu-pid** keyword when connecting to devices such as ATM digital subscriber line (DSL) modems that send PVST (or 802.1D) BPDUs with a PID of 0x00-07.

The **pvst-tlv** keyword enables BPDU translation when the router interoperates with devices that understand only PVST or IEEE Spanning Tree Protocol. Because the Catalyst 6500 series switch ATM modules support PVST+ only, you must use the **pvst-tlv** keyword when connecting to a Catalyst 5000 family switch that understands only PVST on its ATM modules, or when connecting with other Cisco IOS routers that understand IEEE format only.

When the router or switch is transmitting, the **pvst-tlv** keyword translates PVST+ BPDUs into IEEE BPDUs.

When the router or switch is receiving, the **pvst-tlv** keyword translates IEEE BPDUs into PVST+ BPDUs.



Note The **bridge-domain**and **bre-connect** commands are mutually exclusive. You cannot use both commands on the same PVC for concurrent RFC 1483 and BRE bridging.

To preserve class of service (CoS) information across the ATM network, use the **dot1q** option. This configuration uses IEEE 802.1Q tagging to preserve the VLAN ID and packet headers as they are transported across the ATM network.

To enable service providers to use a single VLAN to support customers that have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different customer VLANs, use the **dot1q-tunnel** option on the service provider router. Then use the **dot1q** option on the customer routers.



Note The **access**, **dot1q**, and **dot1q-tunnel** options are mutually exclusive. If you do not specify any of these options, the connection operates in “raw” bridging access mode, which is similar to access, except that the connection does act on and transmit BPDU packets.

RFC 1483 bridging is supported on AAL5-MUX and AAL5-LLC Subnetwork Access Protocol (SNAP) encapsulated PVCs. RFC-1483 bridged PVCs must terminate on the ATM interface, and the bridged traffic must be forwarded over an Ethernet interface, unless the **split-horizon** option is used, which allows bridging of traffic across bridged PVCs.

Note RFC 1483 bridging is not supported for switched virtual circuits (SVCs). It also cannot be configured for PVCs on the main interface.

In interface configuration mode, only the **dot1q** and **dot1q-tunnel** keyword options are supported.

Examples

The following example shows a PVC being configured for IEEE 802.1Q VLAN bridging using a VLAN ID of 99:

```
Router# configure terminal

Router(config)# interface ATM6/2

Router(config-if)# pvc 2/101

Router(config-if-atm-vc)# bridge-domain 99 dot1q

Router(config-if-atm-vc)# end
```

The following example shows how to enable BPDU translation when a Catalyst 6500 series switch is connected to a device that understands only IEEE BPDUs in an RFC 1483-compliant topology:

```
Router(config-if-atm-vc)# bridge-domain
100 pvst-tlv 150
```

The **ignore-bpdu-pid** keyword is not used because the device operates in an RFC 1483-compliant topology for IEEE BPDUs.

The following example shows how to enable BPDU translation when a Catalyst 5500 ATM module is a device that understands only PVST BPDUs in a non-RFC1483-compliant topology. When a Catalyst 6500 series switch is connected to a Catalyst 5500 ATM module, you must enter both keywords.

```
Router(config-if-atm-vc)# bridge-domain
100 ignore-bpdu-pid pvst-tlv 150
```

To enable BPDU translation for the Layer 2 Protocol Tunneling (L2PT) topologies, use the following command:

```
Router(config-if-atm-vc)# bridge-domain
100 dot1q-tunnel ignore-bpdu-pid pvst-tlv 150
```

The following example shows a range of PVCs being configured, with the bridge domain number being incremented for each PVC in the range:

```
Router(config)# interface atm 8/0.100

Router(config-if)# range pvc 102/100 102/199
Router(config-if-atm-range)# bridge-domain 102 increment
```

Related Commands

Command	Description
bre-connect	Enables the BRE over a PVC or SVC.

Command	Description
show atm pvc	Displays the configuration of a particular PVC.

bridge-domain (subinterface)

To enable bridging across Gigabit Ethernet subinterfaces, use the **bridge-domain**command in subinterface configuration mode. To disable bridging, use the **no** form of this command.

bridge-domain *vlan-id* {**dot1q** | **dot1q-tunnel**} [**bpdu** {**drop** | **transparent**}] [**split-horizon**]
no bridge-domain *vlan-id* {**dot1q** | **dot1q-tunnel**} [**bpdu** {**drop** | **transparent**}] [**split-horizon**]

Syntax Description

vlan-id	Specifies the number of the virtual LAN (VLAN) to be used in this bridging configuration. The valid range is from 2 to 4094.
dot1q	Enables IEEE 802.1Q tagging to preserve the class of service (CoS) information from the Ethernet frames across the ATM network. If not specified, the ingress side assumes a CoS value of 0 for QoS purposes.
dot1q-tunnel	Enables IEEE 802.1Q tunneling mode, so that service providers can use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated.
bpdu {**drop** | **transparent**}	(Optional) Specifies whether or not BPDUs are processed or dropped: • **drop** --Specifies that BPDU packets are dropped on the subinterface. • **transparent** --Specifies that BPDU packets are forwarded as data on the subinterface, but not processed.
split-horizon	(Optional) Enables RFC 1483 split horizon mode to globally prevent bridging between PVCs in the same VLAN.

Command Default

Bridging is disabled.

Command Modes

Subinterface configuration (config-subif)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.

Usage Guidelines

This command has the following restrictions in Cisco IOS Release 12.2(33)SRA:

- The command is available on the Cisco 7600 SIP-400 with a 2-Port Gigabit Ethernet SPA only.
- You can place up to 120 subinterfaces in the same bridge domain on a single Cisco 7600 SIP-400.

To enable service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated, use the **dot1q-tunnel** option on the service provider router. Then use the **dot1q** option on the customer routers.

Examples

The following example shows configuration of IEEE 802.1Q encapsulation for VLANs on Gigabit Ethernet subinterfaces with configuration of multipoint bridging (MPB). The MPB feature requires configuration of 802.1Q encapsulation on the subinterface.

The first subinterface bridges traffic on VLAN 100 and preserves CoS information in the packets by specifying the **dot1q** keyword.

```
Router(config)# interface GigabitEthernet 1/0/1.1
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# bridge-domain 100 dot1q
```

The second subinterface shows bridging of traffic on VLAN 200 in tunneling mode using the **dot1q-tunnel** keyword, which preserves the VLAN IDs of the bridged traffic.

```
Router(config)# interface GigabitEthernet 2/0/2.2
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# bridge-domain 200 dot1q-tunnel
```

The following example shows bridging of traffic from different VLANs on two separate Gigabit Ethernet subinterfaces into the same VLAN. First, the bridging VLAN 100 is created using the **vlan** command. Then, the Gigabit Ethernet subinterfaces implement IEEE 802.1Q encapsulation on VLAN 10 and VLAN 20 and bridge the traffic from those VLANs onto VLAN 100 using the **bridge-domain** command:

```
Router(config)# vlan 100
Router(config-vlan)# exit
!
Router(config)# interface GigabitEthernet 1/0/1.1
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# bridge-domain 100 dot1q
Router(config-subif)# exit
!
Router(config)# interface GigabitEthernet 1/0/2.1
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# bridge-domain 100 dot1q
```

Related Commands

Command	Description
encapsulation dot1q	Enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
vlan	Adds the specified VLAN IDs to the VLAN database and enters VLAN configuration mode.