hello

To configure the interval used to exchange hello keepalive packets in a Layer 2 control channel, use the **hello** command in L2TP class configuration mode. To disable the sending of hello keepalive packets, use the **no** form of this command.

hello *seconds*

no hello *seconds*

Syntax Description

seconds	Number of seconds that a router at one end of a Layer 2 control channel waits before sending a hello keepalive packet to its peer router. The valid values range from 0 to 1000 seconds. The default value is 60 seconds.

Defaults

60 seconds

Command Modes

L2TP class configuration

Command History

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

Usage Guidelines

You can configure different values with the **hello** command on the router at each end of a Layer 2 control channel.

Examples

The following example sets an interval of 120 seconds between sendings of hello keepalive messages in pseudowires that have been configured using the L2TP class configuration named "l2tp class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# hello 120
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.

hidden

To hide the attribute-value pair (AVP) values in Layer 2 Tunneling Protocol (L2TP) control messages, use the **hidden** command in L2TP class configuration mode. To unhide AVPs, use the **no** form of this command.

hidden

no hidden

Syntax Description

This command has no arguments or keywords.

Defaults

L2TP AVP hiding is disabled.

Command Modes

L2TP class configuration

Command History

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

Usage Guidelines

Use the **hidden** command to provide additional security for the exchange of control messages between provider edge routers in a Layer 2 Tunnel Protocol Version 3 (L2TPv3) control channel. Because username and password information is exchanged between devices in clear text, it is useful to encrypt L2TP AVP values with the **hidden** command.

Examples

The following example enables AVP hiding and encrypts AVPs in control messages in L2TPv3 pseudowires that have been configured using the L2TP class configuration named "l2tp class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# hidden
```

Related Commands

Command	Description
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.

hostname (L2TP)

To configure the host name that the router will use to identify itself during Layer 2 Tunnel Protocol Version 3 (L2TPv3) authentication, use the **hostname** command in L2TP class configuration mode. To remove the host name, use the **no** form of this command.

hostname *name*

no hostname *name*

Syntax Description

name	Name used to identify the router during authentication.

Defaults

No host name is specified for L2TPv3 authentication.

Command Modes

L2TP class configuration

Command History

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

Usage Guidelines

If you do not use the **hostname** command, the host name of the router is used for L2TPv3 authentication.

Examples

The following example configures the host name "yb2" for a provider edge router used at one end of an L2TPv3 control channel in an L2TPv3 pseudowire that has been configured using the L2TP class configuration named "l2tp class1":

```
Router(config)# l2tp-class l2tp-class1
Router(config-l2tp-class)# hostname yb2
```

Related Commands

Command	Description
ip local interface	Configures the IP address of the PE router interface to be used as the source IP address for sending tunneled packets.
l2tp-class	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.

idle-timeout

To configure the idle timeout parameter for tearing down an ATM switched virtual circuit (SVC) connection, use the **idle-timeout** command in the appropriate command mode. To disable the timeout parameter, use the **no** form of this command.

idle-timeout *seconds* [*minimum-rate*]

no idle-timeout *seconds* [*minimum-rate*]

Syntax Description

seconds	Number of seconds that the SVC is idle, after which the ATM SVC is disconnected.
minimum-rate	(Optional) Minimum traffic rate, in kilobits per second (kbps), required on an ATM SVC to maintain the SVC connection.

Defaults

The default idle timeout is 300 seconds.
The default minimum rate is 0 kbps.

Command Modes

Interface-ATM-VC configuration (for ATM permanent virtual circuits [PVCs] or SVCs)
VC-class configuration (for virtual circuit [VC] classes)

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If within the idle timeout period, both the input and output traffic rates are below the *minimum-rate*, the SVC connection is torn down. The input and output traffic rates are set using the **ubr**, **ubr+**, or **vbr-nrt** command.

If the **idle-timeout** command is not explicitly configured on an ATM SVC, the SVC inherits the following default configuration (listed in order of next highest precedence):

- Configuration of the **idle-timeout** command in a VC class assigned to the SVC itself.
- Configuration of the **idle-timeout** command in a VC class assigned to the SVC's ATM subinterface.
- Configuration of the **idle-timeout** command in a VC class assigned to the SVC's ATM main interface.
- Global default—The global idle timeout default is the value set using the **idle-timeout** interface configuration command. If the **idle-timeout** command is not configured, the default idle timeout is 300 seconds, and the *minimum-rate* is 0 kbps.

Examples

The following example configures an ATM SVC connection inactive after an idle period of 300 seconds. The SVC connection is also configured so that it is considered inactive if the traffic rate is less than 5 kbps.

```
idle-timeout 300 5
```

Related Commands

Command	Description
ubr	Selects UBR QoS and configures the output peak cell rate for an ATM PVC, SVC, or VC class.
ubr+	Selects UBR QoS and configures the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, or VC class.
vbr-nrt	Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, or VC class.

ilmi manage

To enable Integrated Local Management Interface (ILMI) management on an ATM permanent virtual circuit (PVC), use the **ilmi manage** command in the appropriate command mode. To disable ILMI management, use the **no** form of this command.

ilmi manage

no ilmi manage

Syntax Description

This command has no arguments or keywords.

Defaults

ILMI management is disabled.

Command Modes

Interface-ATM-VC configuration (for an ATM PVC)
VC-class configuration (for a virtual circuit [VC] class)
PVC range configuration (for an ATM PVC range)
PVC-in-range configuration (for an individual PVC within a PVC range)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(5)T	This command was made available in PVC range and PVC-in-range configuration modes.

Usage Guidelines

If the **ilmi manage** command is not explicitly configured on an ATM PVC, the PVC inherits the following default configuration (listed in order of precedence):

- Configuration of the **ilmi manage** command in a VC class assigned to the PVC itself.
- Configuration of the **ilmi manage** command in a VC class assigned to the PVC's ATM subinterface.
- Configuration of the **ilmi manage** command in a VC class assigned to the PVC's ATM main interface.
- Global default: ILMI management is disabled.

Examples

The following example enables ILMI management on the ATM PVC with VPI 0 and VCI 60. The ILMI PVC is assigned the name routerA and the VPI and VCI are 0 and 16, respectively.

```
interface atm 0/0
 pvc routerA 0/16 ilmi
 exit
interface atm 0/0.1 multipoint
 pvc 0/60
 ilmi manage
```

ima active-links-minimum

To set the minimum number of links that must be operating in order for an ATM inverse multiplexing over ATM (IMA) group to remain in service, use the **ima active-links-minimum** interface configuration command. To remove the current configuration and set the value to the default, use the **no** form of this command.

ima active-links-minimum *number*

no ima active-links-minimum *number*

Syntax Description

number	Number of links; a value from 1 to 8.

Defaults

Links: 1

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced on Cisco 2600 and 3600 series routers.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.0(5)XE	Support for Cisco 7200 and 7500 series routers was added.
12.0(7)XE1	Support for Cisco 7100 series routers was added.
12.1(5)T	Support for Cisco 7100, 7200, and 7500 series routers was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

The minimum number of links that should be active for continued group operation depends upon the applications you are using and the speeds they require. ATM frame size and the number of links in a group affect the overhead required by ATM.

Examples

The following example specifies that two links in IMA group 2 must be operational in order for the group to remain in service:

```
interface atm 0/ima2
 ima active-links-minimum 2
```

Related Commands

Command	Description
interface atm ima	Configures an ATM IMA group.

ima clock-mode

To set the transmit clock mode for an ATM inverse multiplexing over ATM (IMA) group, use the **ima clock-mode** command in interface configuration mode. To remove the current configuration, use the **no** form of this command.

ima clock-mode {**common** *port* | **independent**}

no ima clock-mode

Syntax Description

common	Sets the transmit clocks for all the links in the group to be derived from the same source.
port	Link that will provide clocking for the IMA group (called the command link). If the common link fails, the system automatically chooses one of the remaining active links to provide clocking.
independent	Sets the transmit clock source for at least one link in the IMA group to be different from the clock source used by the other links.

Defaults

The default value is **common**. If no port is specified, the system automatically chooses an active link to provide clocking.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced on Cisco 2600 and 3600 series routers.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T
12.0(5)XE	This command was implemented on Cisco 7200 and 7500 series routers.
12.0(7)XE1	This command was implemented on Cisco 7100 series routers.
12.1(5)T	Support for Cisco 7100, 7200, and 7500 series routers was implemented in Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command controls the clock for the IMA group as a whole. If all the links in the group share a clock source, use the **common** keyword. If all the links use different clock sources, use the **independent** clock source keyword.

When the **common** keyword is set, the **clock source** ATM interface configuration command for the common link determines clocking for all the links in the group.When the **independent** keyword is set, the **clock source** ATM interface configuration command is used under each interface to determine clocking individually.

Because the system automatically chooses a replacement for the common link when it fails, any link in an IMA group potentially can provide the recovered transmit clock. For this reason, even when the common keyword is set with a specific link stipulated by the port value, you should use the ATM interface configuration **clock source** command to make sure that the clock source is configured correctly on each interface in the IMA group.

Examples

The following example specifies that the links in IMA group 2 use a common clock source on link 0:

```
interface atm0/ima2
 ima clock-mode common 0
```

Related Commands

Command	Description
clock source	Configures the clock source of a DS1 link.
interface atm ima	Configures an ATM IMA group.
show ima interface atm	Provides information about all configured IMA groups or a specific IMA group.

ima differential-delay-maximum

To specify the maximum differential delay among the active links in an inverse multiplexing over ATM (IMA) group, use the **ima differential-delay-maximum** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

ima differential-delay-maximum *milliseconds*

no ima differential-delay-maximum *milliseconds*

Syntax Description

msec	Specifies the differential delay in milliseconds (ms). The range of values depends on the type of card used. PA-A3-8T1IMA—25 to 250 milliseconds PA-A3-8E1IMA—25 to 190 milliseconds NM-8T1-IMA—25 to 200 milliseconds

Defaults

25 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced on Cisco 2600 and 3600 series routers.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.0(5)XE	This command was implemented on Cisco 7200 and 7500 series routers.
12.0(7)XE1	This command was implemented on Cisco 7100 series routers.
12.1(5)T	Support for Cisco 7100, 7200, and 7500 series routers was implemented in Cisco IOS Release 12.1(5)T.

Usage Guidelines

This command helps control latency in ATM-layer traffic by setting a limit on how much latency the slowest link in the group is allowed to introduce (a slower link has a longer propagation delay—for example, due to a longer path through the network or less accurate physical layer clocking—than other links). Setting a high value allows a slow link to continue operating as part of the group, although such a setting means there is added delay to links across the group. A low setting may result in less latency for traffic across the group than a high setting, but it can mean that the system takes a slow link out of operation, reducing total bandwidth.

When a link has been removed from service, it is automatically placed back in service when it meets the delay differential standard. If a link delay exceeds the specified maximum, the link is dropped; otherwise, the IMA feature adjusts for differences in delays so that all links in a group are aligned and carry ATM-layer traffic.

Examples

The following example specifies that the links in IMA group 2 have a maximum differential delay of 50 ms:

```
interface atm0/ima2
 ima differential-delay-maximum 50
```

Related Commands

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

ima frame-length

To specify the number of cells in inverse multiplexing over ATM (IMA) frames, use the **ima frame-length** interface configuration command. To remove the current setting and restore the default value, use the **no** form of this command.

ima frame-length {**32** | **64** | **128** | **256**}

no ima frame-length {**32** | **64** | **128** | **256**}

Syntax Description

32	Specifies a value of 32 cells.
64	Specifies a value of 64 cells.
128	Specifies a value of 128 cells.
256	Specifies a value of 256 cells.

Defaults

The default value is 128 cells in a frame.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)XE1	Support for Cisco 7100 series routers added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

IMA frames are numbered sequentially, and each contains an IMA Control Protocol (ICP) cell at a specific position.

Frame length can affect performance because the greater the total number of frames required to communicate a given number of cells, the greater the overhead for header and other control cells. In addition, shorter frame lengths might diminish performance when translated ATM-Frame Relay interworking occurs.

Examples

On Cisco 7100 and 7200 series routers, the following example specifies that the links in IMA group 2 have a frame length of 64 cells:

```
interface atm 1/ima2
 ima frame-length 64
```

ima test

To specify an interface and test pattern for verifying connectivity of all links in an inverse multiplexing over ATM (IMA) group, use the **ima test** command in interface configuration mode. To stop the test, use the **no** form of this .

ima test [**link** *port*] [**pattern** *pattern-id*]

no ima test [**link** *port*] [**pattern** *pattern-id*]

Syntax Description

link *port*	(Optional) The identifier for the interface where the physical link is located.
pattern *pattern-id*	(Optional) A value from 0 to 254, set in hexadecimal or decimal numbers, identifying a pattern to be sent to the far end of the link.

Defaults

There is no default for the *port* value. The default value for *pattern-id* is 106 (0x6A).

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced on Cisco 2600 and 3600 series routers.
12.0(5)T	This command was integrated into Cisco IOS 12.0(5)T.
12.0(5)XE	Support for Cisco 7200 and 7500 series routers was added.
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.

Usage Guidelines

To verify link and group connectivity, the pattern is sent from the specified link and looped back from the receiving end across all links belonging to the group as defined at the remote end. Verifying link and group connectivity can help troubleshoot physical link connectivity or configuration problems at the remote end. The local end verifies that the pattern is returned on all links belonging to the group at the local end, and testing is continuous. An IMA control protocol (ICP) cell in each frame identifies the pattern.

When a link is not transmitting or receiving a pattern correctly, the command reports the link number where the problem exists.

Examples

The following example configures link 4 to send test pattern 56:

```
interface atm 0/ima 2
 ima test link 2 pattern 56
```

Related Commands

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

ima-group

To define physical links as inverse multiplexing over ATM (IMA) group members, use the **ima-group** command in interface configuration mode for each group member. To remove the port from the group, use the **no** form of this command.

ima-group *group-number*

no ima-group *group-number*

Syntax Description

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

Defaults

Physical links are not included in IMA groups.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced on Cisco 2600 and 3600 series routers.
12.0(5)T	This command was integrated into Cisco IOS 12.0(5)T.
12.0(5)XE	Support for Cisco 7200 and 7500 series routers was added.
12.0(7)XE1	Support for Cisco 7100 series routers was added.
12.1(5)T	Support for Cisco 7100, 7200, and 7500 series routers was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

When the configuration is first performed or when the group number is changed, the interface is automatically disabled, moved to the new group, and then enabled.

Examples

The following example makes interface 1 on the ATM module in slot 0 a member of IMA group 2:

```
interface atm0/1
 ima-group 2
```

Related Commands

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

inarp

To configure the Inverse Address Resolution Protocol (ARP) time period for an ATM permanent virtual circuit (PVC), virtual circuit (VC) class, or VC bundle, use the **inarp** command in the appropriate command mode. To restore the default Inverse ARP time period behavior, use the **no** form of this command.

inarp *minutes*

no inarp *minutes*

Syntax Description

minutes	Number of minutes for the Inverse ARP time period.

Defaults

minutes: 15 minutes.

Command Modes

Interface-ATM-VC configuration (for an ATM PVC)
VC-class configuration (for a VC class)
Bundle configuration (for a VC bundle)
PVC range configuration (for an ATM PVC range)
PVC-in-range configuration (for an individual PVC within a PVC range)

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(3)T	This command was enhanced to provide support to configure the Inverse ARP time period for an ATM VC bundle.
12.1(5)T	This command was made available in PVC range and PVC-in-range configuration modes.

Usage Guidelines

This command is supported for **aal5snap** encapsulation only when Inverse ARP is enabled. Refer to the **encapsulation** command for configuring **aal5snap** encapsulation and the **protocol** command for enabling Inverse ARP.

If the **inarp** command is not explicitly configured on an ATM PVC, the PVC inherits the following default configuration (listed in order of precedence):

- Configuration of the **inarp** command in a VC class assigned to the PVC itself.
- Configuration of the **inarp** command in a VC class assigned to the PVC's ATM subinterface.
- Configuration of the **inarp** command in a VC class assigned to the PVC's ATM main interface.
- Global default for the *minutes* argument is 15 minutes; this default assumes that Inverse ARP is enabled.

Note As the inheritance rules imply, when a VC is a member of a VC bundle, configuration using the **inarp** command in VC-class configuration mode no longer applies to that VC. Bundle configuration takes precedence.

For ATM VC bundle management, the Inverse ARP parameter can only be enabled at the bundle level and applied to all VC members of the bundle—that is, it cannot be enabled in bundle-vc configuration mode for individual VC bundle members. To use this command in bundle configuration mode, first enter the **bundle** command to create the bundle and enter bundle configuration mode.

Examples

The following example sets the Inverse ARP time period to 10 minutes:

```
inarp 10
```

Related Commands

Command	Description
bundle	Creates a bundle or modifies an existing bundle to enter bundle configuration mode.
broadcast	Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle.
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.
encapsulation atm-dxi	Configures the AAL and encapsulation type for an ATM PVC, SVC, or VC class.
oam-bundle	Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle.
oam retry	Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle.
protocol (ATM)	Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only).

inarp (Frame Relay VC-bundle-member)

To override the default permanent virtual circuit (PVC) bundle member used for Inverse Address Resolution Protocol (ARP) and specify a different PVC bundle member to handle the Inverse ARP packets, use the **inarp** command in Frame Relay VC-bundle-member configuration mode. To disable Inverse ARP on the PVC bundle member, use the **no** form of this command.

inarp

no inarp

Syntax Description

This command has no arguments or keywords.

Defaults

Inverse ARP is handled by the PVC that handles precedence or EXP level 6 or DSCP level 63.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.

Usage Guidelines

In each Frame Relay PVC bundle, Inverse ARP by default is handled by the PVC that handles precedence or EXP level 6 or DSCP level 63. In the default case, if the PVC handling Inverse ARP traffic goes down, the Inverse ARP packets are diverted to the PVC that has been configured to handle the bumped traffic for precedence level 6 or DSCP level 63.

Inverse ARP packets arriving on PVCs that are not configured to handle Inverse ARP will be dropped.

If you override the default packet service levels and enable Inverse ARP on a PVC that handles a different precedence or DSCP level, and that PVC goes down, the Inverse ARP packets will be dropped even if another PVC accepts the bumped traffic from the failed PVC.

If the **inarp** command is entered on two different PVC bundle members, Inverse ARP traffic will be handled by the second entry.

Examples

The following example shows Inverse ARP enabled on PVC 250, which handles DSCP level 60:

```
interface serial 1/4.1 multipoint
 frame-relay vc-bundle MP-4-dynamic
  match dscp
  pvc 100
   dscp other
  pvc 250
   dscp 60
   inarp
```

Related Commands

Command	Description
dscp (Frame Relay VC-bundle-member))	Configures the DSCP value or values for a Frame Relay PVC bundle member.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.

interface atm

To configure an ATM interface and enter interface configuration mode, use the **interface atm** command in global configuration mode.

interface atm *interface-number*[**.***subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]

Syntax Description

interface-number	Specifies a (physical) ATM interface (for example, 3/0).
.*subinterface-number*	(Optional) Specifies a subinterface number. A dot (.) must be used to separate the *interface-number* from the *subinterface-number* (for example 2/0.1).
mpls	(Optional) Specifies MPLS as the interface type for which a subinterface is to be created.
multipoint	(Optional) Specifies multipoint as the interface type for which a subinterface is to be created.
point-to-point	(Optional) Specifies point-to-point as the interface type for which a subinterface is to be created.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	New optional subinterface types were introduced.

Usage Guidelines

The **interface atm** command enables you to define a subinterface for a specified type of ATM interface. The subinterface for the ATM interface is created the first time this command is issued with a specified subinterface number.

Examples

For physical ATM interface 3/0, the following command creates an ATM MPLS subinterface having subinterface number 1:

```
Router# interface atm 3/0.1 mpls
```

Related Commands

Command	Description
show interfaces atm	Displays information about the ATM interface.
show mpls interfaces	Displays information about one or more MPLS interfaces that have been configured for label switching.

interface atm ima

To configure an inverse multiplexing over ATM (IMA) group, use the **interface atm ima** global configuration command.

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

Syntax Description

slot/	Specifies the slot location of the ATM IMA network module. The values range from 0 to 5 depending on the router.
group-number	Enter an IMA group number from 0 to 3. You can create up to four groups. Do not include a space before the group number.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XK	This command was introduced on Cisco 2600 and 3600 series routers.
12.0(5)T	This command was integrated into Cisco IOS 12.0(5)T.
12.0(5)XE	Support for Cisco 7200 and 7500 series routers was added.
12.0(7)XE1	Support for Cisco 7100 series routers was added.
12.1(5)T	Support for Cisco 7100, 7200, and 7500 series routers was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

If the group does not exist when the command is issued, the command automatically creates the group.

When a port is configured for IMA functionality, it no longer operates as an individual ATM link.

Specifying ATM links as members of a group by using the **ima group** interface command does not enable the group. You must use the **interface atm ima** command to create the group.

Examples

The following example configures IMA group 0 on the module in slot 1:

```
interface atm 1/ima0
  ip address 10.18.16.121 255.255.255.192
```

Related Commands

Command	Description
ima-group	Defines IMA group members.
interface atm	Configures an ATM interface.

Command	Description
show ima interface atm	Provides information about all configured IMA groups or a specific IMA group.
shutdown (interface)	Disables an interface.

interface cbr

To specify the T1 or E1 constant bit rate interface on an ATM-CES port adapter, and to enter interface configuration mode, use the **interface cbr** command in global configuration mode.

interface cbr *slot*/*port*

Syntax Description

slot/	Backplane slot number. The slash (/) must be typed.
port	Interface port number.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The ATM-CES port adapter has four T1 (1.544 Mbps) or four E1 (2.048 Mbps) ports (75- or 120-ohm) that can support both structured (N x 64 kbps) and unstructured ATM Forum-compliant circuit emulation services (CES), and one port that supports an OC-3 (155 Mbps) single-mode intermediate reach interface or a T3 (45 Mbps) or E3 (34 Mbps) standards-based ATM interface.

Examples

The following example specifies the first T1 or E1 port on the ATM-CES port adapter in slot 1:

```
interface cbr 1/0
```

Related Commands

Command	Description
show ces interface cbr	Displays detailed CBR port information.
show interface cbr	Displays the information about the CBR interface on the ATM-CES port adapter.

interface fr-atm

To create a Frame Relay-ATM Interworking interface on the Cisco MC3810 and to enter Frame Relay-ATM Interworking configuration mode, use the **interface fr-atm** global configuration command. To delete the Frame Relay-ATM Interworking interface, use the **no** form of this command.

interface fr-atm *number*

no interface fr-atm *number*

Syntax Description

number	The Frame Relay-ATM Interworking interface number. Range is from 0 to 20.

Defaults

Frame Relay-ATM Interworking interface 20 is configured by default.

Command Modes

Global configuration

Command History

Release	Modification
11.3 MA	This command was introduced.

Usage Guidelines

This command applies to Frame Relay-ATM Interworking on the Cisco MC3810 only.

Use the **interface fr-atm** command to enter Frame Relay-ATM interworking interface configuration mode. When you issue this command for the first time, an interface number is created dynamically. You can configure up to 21 Frame Relay-ATM interworking interfaces.

Note The Cisco MC3810 provides only *network interworking* (FRF.5). The Cisco MC3810 can be used with *service interworking* (FRF.8), which is provided by the carrier's ATM network equipment.

Examples

The following example configures Frame Relay-ATM Interworking interface number 20:

```
interface fr-atm 20
```

Related Commands

Command	Description
fr-atm connect dlci	Maps a Frame Relay DLCI to an ATM virtual circuit descriptor for FRF.5 Frame Relay-ATM internetworking.

interface mfr

To configure a multilink Frame Relay bundle interface, use the **interface mfr** command in global configuration mode. To remove the bundle interface, use the **no** form of this command.

interface mfr *number*

no interface mfr *number*

Syntax Description

number	Number that will uniquely identify this bundle interface. Range is from 0 to 2147483647.

Defaults

A bundle interface is not configured.
Frame Relay encapsulation is the default encapsulation type for multilink Frame Relay bundle interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.0(24)S	This command was introduced on VIP-enabled Cisco 7500 series routers.
12.3(4)T	Support for this command on VIP-enabled Cisco 7500 series routers was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A bundle interface is a virtual interface that serves as the Frame Relay data link and performs the same functions as a physical interface. The bundle is made up of physical serial links, called bundle links. The bundle links within a bundle function as one physical link and one pool of bandwidth. Functionality that you want to apply to the bundle links must be configured on the bundle interface.

The **no interface mfr** command will work only if all bundle links have been removed from the bundle by using the **no encapsulation frame-relay mfr** command.

Examples

The following example shows the configuration of a bundle interface called “mfr0”. The bundle identification (BID) name “BUNDLE-A” is assigned to the bundle. Serial interfaces 0 and 1 are assigned to the bundle as bundle links.

```
interface mfr0
 frame-relay multilink bid BUNDLE-A
!
interface serial0
 encapsulation frame-relay mfr0
!
interface serial1
 encapsulation frame-relay mfr0
```

Related Commands

Command	Description
debug frame-relay multilink	Displays debug messages for multilink Frame Relay bundles and bundle links.
encapsulation frame-relay mfr	Creates a multilink Frame Relay bundle link and associates the link with a bundle.
frame-relay multilink bid	Assigns a BID name to a multilink Frame Relay bundle.
show frame-relay multilink	Displays configuration information and statistics about multilink Frame Relay bundles and bundle links.

interface serial multipoint

To define a logical subinterface on a serial interface to support multiple logical IP subnetworks over Switched Multimegabit Data Service (SMDS), use the **interface serial multipoint** interface configuration command.

interface serial {*interface* | *slot/port*}**.***subinterface* **multipoint**

Syntax Description

interface	Interface number.
slot/port	Slot and port number related to specified subinterface (for Cisco 7000 and 7500 series routers).
.*subinterface*	Number for this subinterface; values in the range 0 to 255.

Defaults

This command has no default values.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command only for routers that need knowledge of multiple IP networks. Other routers can be configured with information only about their own networks. A period must be used to separate the *interface* or *slot/port* from the *subinterface*.

Examples

The following example configures serial interface 2 with multipoint logical subinterface 1:

```
interface serial 2.1 multipoint
```

The following example configures slot 2 port 0 with multipoint logical subinterface 1:

```
interface serial 2/0.1 multipoint
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
smds address	Specifies the SMDS individual address for a particular interface.
smds enable-arp	Enables dynamic ARP.The multicast address for ARP must be set before this command is issued.
smds multicast	Assigns a multicast SMDS E.164 address to a higher-level protocol.

ip dfbit set

To enable the Don't Fragment (DF) bit in the outer Layer 2 header, use the **ip dfbit set** command in pseudowire class configuration mode. To disable the DF bit setting, use the **no** form of this command.

ip dfbit set

no ip dfbit set

Syntax Description

This command has no arguments or keywords.

Defaults

For Cisco 12000 series Internet routers, the DF bit is on by default.

For other platforms, the DF bit is off by default.

Command Modes

Pseudowire class configuration

Command History

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

Usage Guidelines

Use this command to set the DF bit on if, for performance reasons, you do not want tunneled packet reassembly to be performed on the router.

Note The **no ip dfbit set** command is not supported on the Cisco 12000 series Internet routers.

Examples

The following example shows how to enable the DF bit in the outer Layer 2 header in pseudowires that were created from the pseudowire class named "ether-pw":

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip dfbit set
```

Related Commands

Command	Description
ip pmtu (L2TP)	Enables the discovery of a PMTU for Layer 2 traffic.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

ip local interface

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

ip local interface *interface-name*

no ip local interface *interface-name*

Syntax Description

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

Defaults

No IP address is configured.

Command Modes

Pseudowire class configuration

Command History

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

Usage Guidelines

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

Note The interface configured with the **ip local interface** command must be a loopback interface on Cisco 12000 series Internet routers.

Note This command must be configured for pseudowire class configurations using Layer 2 Tunnel Protocol version 3 (L2TPv3) as the data encapsulation method.

Examples

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

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip local interface ethernet 0/0
```

Related Commands

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

ip pmtu

To enable the discovery of a path maximum transmission unit (MTU) for Layer 2 traffic, use the **ip pmtu** command in VPDN group configuration mode or pseudowire class configuration mode. To disable path MTU discovery, use the **no** form of this command.

ip pmtu

no ip pmtu

Syntax Description

This command has no arguments or keywords.

Defaults

Path MTU discovery is disabled.

Command Modes

VPDN group configuration
Pseudowire class configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Usage Guidelines

When issued in VPDN group configuration mode, the **ip pmtu** command enables any Layer 2 Tunnel Protocol (L2TP) tunnel associated with the specified virtual private dial-up network (VPDN) group to participate in path MTU discovery.

When issued in pseudowire class configuration mode, the **ip pmtu** command enables any Layer 2 session derived from the specified pseudowire class configuration to participate in path MTU discovery.

Path MTU checks decrease switching performance; therefore this option is disabled by default.

The **ip pmtu** command enables the processing of Internet Control Message Protocol (ICMP) unreachable messages that indicate fragmentation errors in the IP backbone network carrying the tunneled traffic. The MTU of the Layer 2 session is updated according to the MTU information contained in the ICMP unreachable message.

The **ip pmtu** command also enables MTU checking for IP packets that are sent into a Layer 2 session with the Don't Fragment (DF) bit set. If an IP packet is larger than the MTU of the tunnel, the packet is dropped and an ICMP unreachable message is sent. If an IP packet is smaller than the MTU of the tunnel, the DF bit in the packet header is reflected from the inner IP header to the tunnel header.

Examples

The following example configures a VPDN group named "dial-in" on an L2TP network server and uses the **ip pmtu** command to specify that L2TP tunnels will participate in path MTU discovery:

```
vpdn-group dial-in
```

```
 accept-dialin
  protocol l2tp
  virtual-template 1
 l2tp security crypto-profile l2tp
 no l2tp tunnel authentication
 lcp renegotiation on-mismatch
 ip pmtu
```

The following example shows how to enable the discovery of the path MTU for pseudowires that have been created from the pseudowire class named “ether-pw”:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip pmtu
```

Related Commands

Command	Description
ip dfbit set	Enables the DF bit in the outer Layer 2 tunnel header.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

ip protocol

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

ip protocol {**l2tp** | **uti** | *protocol-number*}

no ip protocol {**l2tp** | **uti** | *protocol-number*}

Syntax Description

l2tp	Configures L2TP as the IP protocol used to tunnel packets in a Layer 2 pseudowire. This is the default.
uti	Configures UTI as the IP protocol used to tunnel packets in a Layer 2 pseudowire, and allows a router running L2TP version 3 (L2TPv3) to interoperate with a peer running UTI.
protocol-number	The protocol number of the desired IP protocol. The protocol number for L2TPv3 is 115. The protocol number for UTI is 120.

Defaults

The default IP protocol is L2TP.

Command Modes

Pseudowire class configuration

Command History

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

Usage Guidelines

Use the **ip protocol** command to ensure backward compatibility with routers running UTI. This command allows you to configure an L2TPv3 pseudowire between a router running L2TPv3 and a peer router running UTI.

Note You can use the **ip protocol** command only if you have already entered the **encapsulation l2tpv3** command.

To configure L2TP as the IP protocol that is used to tunnel packets in an L2TPv3 pseudowire, you may enter **115**, the IP protocol number assigned to L2TPv3, instead of **l2tp** in the **ip protocol** command.

To configure UTI as the IP protocol that is used to tunnel packets in an L2TPv3 pseudowire, you may enter **120**, the IP protocol number assigned to UTI, instead of **uti** in the **ip protocol** command.

Note Interoperability in an L2TPv3 control channel between a router running UTI and a router configured for L2TPv3 encapsulation is supported only if you disable signaling using the **protocol none** command.

Examples

The following example shows how to configure UTI as the IP protocol used to tunnel packets in an L2TPv3 pseudowire created from the pseudowire class named “ether-pw”:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# encapsulation l2tpv3
Router(config-pw)# ip protocol uti
```

Related Commands

Command	Description
encapsulation (L2TP)	Configures the Layer 2 data encapsulation method used to tunnel IP traffic.
protocol (L2TP)	Specifies the signaling protocol to be used to manage the pseudowires created from a pseudowire class for a Layer 2 session, and that control plane configuration settings are to be taken from a specified L2TP class.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.

ip tcp adjust-mss

To adjust the maximum segment size (MSS) value of TCP SYN packets going through a router, use the **ip tcp adjust-mss** command in interface configuration mode. To return the MSS value to the default setting, use the **no** form of this command.

ip tcp adjust-mss *max-segment-size*

no ip tcp adjust-mss *max-segment-size*

Syntax Description

max-segment-size	Maximum segment size, in bytes. The range is from 500 to 1460.

Defaults

If the **ip tcp adjust-mss** command is not configured, the MSS is determined by the originating host.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was changed from **ip adjust-mss** to **ip tcp adjust-mss**.

Usage Guidelines

When a host (usually a PC) initiates a TCP session with a server, it negotiates the IP segment size by using the MSS option field in the TCP SYN packet. The value of the MSS field is determined by the maximum transmission unit (MTU) configuration on the host. The default MSS value for a PC is 1500 bytes.The PPP over Ethernet (PPPoE) standard supports a MTU of only 1492 bytes. The disparity between the host and PPPoE MTU size can cause the router in between the host and the server to drop 1500-byte packets and terminate TCP sessions over the PPPoE network. Even if the path MTU (which detects the correct MTU across the path) is enabled on the host, sessions may be dropped because system administrators sometimes disable the ICMP error messages that must be relayed from the host in order for path MTU to work.

The **ip tcp adjust-mss** command helps prevent TCP sessions from being dropped by adjusting the MSS value of the TCP SYN packets.

The **ip tcp adjust-mss** command is effective only for TCP connections passing through the router.

In most cases, the optimum value for the *max-segment-size* argument is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.

If you are configuring the **ip mtu** command on the same interface as the **ip tcp adjust-mss** command, it is recommended that you use the following commands and values:

- **ip tcp adjust-mss 1452**
- **ip mtu 1492**

Examples

The following example shows the configuration of a PPPoE client with the MSS value set to 1452:

```
vpdn enable
no vpdn logging
!
vpdn-group 1
request-dialin
protocol pppoe
!
interface Ethernet0
 ip address 192.168.100.1.255.255.255.0
 ip tcp adjust-mss 1452
 ip nat inside
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 8/35
 pppoe client dial-pool-number 1
!
dsl equipment-type CPE
dsl operating-mode GSHDSL symmetric annex B
dsl linerate AUTO
!
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication pap callin
 ppp pap sent-username sohodyn password 7 141B1309000528
!
ip nat inside source list 101 Dialer1 overload
ip route 0.0.0.0.0.0.0.0 Dialer1
access-list permit ip 192.168.100.0.0.0.0.255 any
```

Related Commands

Command	Description
ip mtu	Sets the MTU size of IP packets sent on an interface.

ip tos (L2TP)

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

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

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

Syntax Description

value *value*	Sets the value of the ToS byte for IP packets in a Layer 2 Tunnel Protocol version 3 (L2TPv3) session. Valid values range from 0 to 255. The default value is 0.
reflect	Sets the value of the ToS byte for IP packets in an L2TPv3 session to be reflected from the inner IP header.

Defaults

The default ToS value is 0.

Command Modes

Pseudowire class configuration

Command History

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

Usage Guidelines

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

Note The **reflect** option is not supported on the Cisco 10720 and Cisco 12000 series Internet routers.

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

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

Examples

In the following example, the ToS byte in the headers of tunneled packets in Layer 2 tunnels created from the pseudowire class named “ether-pw” will be reflected from the ToS value in the header of each encapsulated IP packet:

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip tos reflect
```

Related Commands

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

ip ttl

To configure the time-to-live (TTL) byte in the IP headers of Layer 2 tunneled packets, use the **ip ttl** command in pseudowire class configuration mode. To remove the configured TTL value, use the **no** form of this command.

ip ttl *value*

no ip ttl *value*

Syntax Description

value	Value of the TTL byte in the IP headers of L2TPv3 tunneled packets. The valid values range from 1 to 255. The default value is 255.

Defaults

value: 255

Command Modes

Pseudowire class configuration

Command History

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

Usage Guidelines

Use this command to set the Don't Fragment (DF) bit on if, for performance reasons, you do not want tunneled packet reassembly to be performed on the router.

Examples

The following example shows how to set the TTL byte to 100 in the IP header of Layer 2 tunneled packets in pseudowires that were created from the pseudowire class named "ether-pw":

```
Router(config)# pseudowire-class ether-pw
Router(config-pw)# ip ttl 100
```

Related Commands

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

keepalive (LMI)

To enable the Local Management Interface (LMI) mechanism for serial lines using Frame Relay encapsulation, use the **keepalive** interface configuration command. To disable this capability, use the **no** form of this command.

keepalive *number*

no keepalive

Syntax Description

number	Number of seconds that defines the keepalive interval. The interval must be set as a positive integer that is less than the interval set on the switch; see the **frame-relay lmi-t392dce** command description earlier in this chapter.

Defaults

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **keepalive** command enables the keepalive sequence, which is part of the LMI protocol.

Note When booting from a network server over Frame Relay, you might need to disable keepalives.

Examples

The following example sets the keepalive timer on the server for a period that is two or three seconds faster (has a shorter interval) than the interval set on the keepalive timer of the Frame Relay switch. The difference in keepalive intervals ensures proper synchronization between the Cisco server and the Frame Relay switch.

```
interface serial 3
 keepalive 8
```

Related Commands

Command	Description
frame-relay lmi-t392dce	Sets the polling verification timer on a DCE or NNI interface.

l2tp cookie local

To configure the size of the cookie field used in the Layer 2 Tunnel Protocol Version 3 (L2TPv3) headers of incoming packets received from the remote provider edge (PE) peer router, use the **l2tp cookie local** command in xconnect configuration mode. To remove the configured cookie field parameters, use the **no** form of this command.

l2tp cookie local *size low-value* [*high-value*]

no l2tp cookie local *size low-value* [*high-value*]

Syntax Description

size	The size of the cookie field in L2TPv3 headers. The valid values are 0, 4, and 8.
low-value	The value of the lower 4 bytes of the cookie field.
high-value	(Optional) The value of the upper 4 bytes of the cookie field. For 8-byte cookie fields, you must enter the value for the upper 4 bytes of the cookie field.

Defaults

No cookie value is included in the header of L2TP packets.

Command Modes

Xconnect configuration

Command History

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

Usage Guidelines

The **l2tp cookie local** command specifies the values that the peer PE router includes in the cookie field in L2TPv3 headers of the packets it sends to the local PE router through an L2TPv3 session. These values are required in a static L2TPv3 session.

The cookie field is an optional part of an L2TPv3 header with a length of either 4 or 8 bytes. If you specify an 8-byte length, you must also enter a value for the *high-value* argument.

Note For the Cisco 10720 and Cisco 12000 series Internet routers, an 8-byte cookie must be configured with this command.

Examples

The following example shows how to configure the cookie field of 4 bytes starting at 54321 for the L2TPv3 headers in incoming tunneled packets that were sent from the remote PE peer:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp cookie local 4 54321
```

Related Commands

Command	Description
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing (sent) packets from the remote PE peer router.
l2tp hello	Configures the interval between hello keepalive messages.
l2tp id	Configures the IDs used by the local and remote PE routers at each end of an L2TPv3 session.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp cookie remote

To configure the size of the cookie field used in the Layer 2 Tunnel Protocol Version 3 (L2TPv3) headers of outgoing packets sent from the local provider edge (PE) peer router, use the **l2tp cookie remote** command in xconnect configuration mode. To remove the configured cookie field parameters, use the **no** form of this command.

l2tp cookie remote *size low-value* [*high-value*]

no l2tp cookie remote *size low-value* [*high-value*]

Syntax Description

size	The size of the cookie field in L2TPv3 headers. The valid values are 0, 4, and 8.
low-value	The value of the lower 4 bytes of the cookie field.
high-value	(Optional) The value of the upper 4 bytes of the cookie field. For 8-byte cookie fields, you must enter the value for the upper 4 bytes of the cookie field.

Defaults

No cookie value is included in the header of L2TP packets.

Command Modes

Xconnect configuration

Command History

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

Usage Guidelines

The **l2tp cookie remote** command specifies the values that the local PE router includes in the cookie field in L2TPv3 headers of the packets it sends to the remote PE router through an L2TPv3 session. These values are required in a static L2TPv3 session.

The cookie field is an optional part of an L2TPv3 header with a length of either 4 or 8 bytes. If you specify an 8-byte length, you must also enter a value for the *high-value* argument.

Examples

The following example shows how to configure the cookie field of 4 bytes starting at 12345 for the L2TPv3 headers in outgoing tunneled packets sent to the remote PE peer:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp cookie remote 4 12345
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming (received) packets from the remote PE peer router.
l2tp hello	Configures the interval between hello keepalive messages.
l2tp id	Configures the IDs used by the local and remote PE routers at each end of an L2TPv3 session.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp hello

To specify the use of a hello keepalive setting contained in a specified Layer 2 Tunneling Protocol class configuration for a static Layer 2 Tunnel Protocol Version 3 (L2TPv3) session, use the **l2tp hello** command in xconnect configuration mode. To disable the sending of hello keepalive messages, use the **no** form of this command.

l2tp hello *l2tp-class-name*

no l2tp hello *l2tp-class-name*

Syntax Description

l2tp-class-name	Specifies the L2TP class configuration in which the hello keepalive interval to be used for the L2TPv3 session is stored.

Defaults

No hello keepalive messages are sent.

Command Modes

Xconnect configuration

Command History

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

Usage Guidelines

Because a static L2TPv3 session does not use a control plane to dynamically negotiate control channel parameters, you must use the **l2tp hello** command to specify an L2TP class configuration that contains the interval for sending hello keepalive messages.

Examples

The following example shows how to configure the time interval for hello keepalive messages stored in the L2TP class configuration named "l2tp-default"s for an Ethernet interface using the configuration settings stored in the pseudowire class named "ether-pw":

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp hello lt2p-defaults
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming (received) packets from the remote PE peer router.
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing (transmitted) packets from the remote PE peer router.

Command	Description
l2tp id	Configures the IDs used by the local and remote PE routers at each end of an L2TPv3 session.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp id

To configure the identifiers used by the local and remote provider edge (PE) routers at each end of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) session, use the **l2tp id** command in xconnect configuration mode. To remove the configured identifiers for local and remote sessions, use the **no** form of this command.

l2tp id *local-session-ID remote-session-ID*

no l2tp id *local-session-ID remote-session-ID*

Syntax Description

local-session-ID	The identifier used by the local PE router as its local session identifier.
remote-session-ID	The identifier used by the remote PE router as its local session identifier.

Defaults

No session identifiers are configured.

Command Modes

Xconnect configuration

Command History

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

Usage Guidelines

The xconnect configuration that binds an attachment circuit to an L2TPv3 pseudowire is not complete without configured values for the *local-session-ID* and *remote-session-ID* arguments.

Examples

The following example shows how to configure the identifiers named “222” for the local PE router and “111” for the remote peer in an L2TPv3 session bound to an Ethernet circuit using the L2TPv3 configuration settings stored in the pseudowire class named” ether-pw”:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn)# l2tp id 222 111
```

Related Commands

Command	Description
l2tp cookie local	Configures the size of the cookie field used in the L2TPv3 headers of incoming (received) packets from the remote PE peer router.
l2tp cookie remote	Configures the size of the cookie field used in the L2TPv3 headers of outgoing (transmitted) packets from the remote PE peer router.

Command	Description
l2tp hello	Configures the interval between hello keepalive messages.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

l2tp-class

To create a template of Layer 2 Tunnel Protocol (L2TP) control plane configuration settings that can be inherited by different pseudowire classes and to enter L2TP class configuration mode, use the **l2tp-class** command in global configuration mode.

l2tp-class [*l2tp-class-name*]

Syntax Description

l2tp-class-name	(Optional) Name of the L2TP class. The *name* argument must be specified if you want to configure multiple sets of L2TP control parameters.

Defaults

No L2TP classes are defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **l2tp-class** *l2tp-class-name* command allows you to configure an L2TP class template that consists of configuration settings used by different pseudowire classes. An L2TP class includes the following configuration settings:

- Host name of local router used during Layer 2 authentication
- Authentication enabled
- Time interval used for exchange of hello packets
- Password used for control channel authentication
- Packet size of receive window
- Retransmission settings for control packets
- Time allowed to set up a control channel

The **l2tp-class** command enters L2TP class configuration mode, where L2TP control plane parameters are configured.

You must use the same L2TP class in the pseudowire configuration at both ends of a Layer 2 control channel.

Examples

The following example shows how to enter L2TP class configuration mode to create an L2TP class configuration template for the class named “ether-pw”:

```
Router(config)# l2tp-class ether-pw
Router(config-l2tp-class)#
```

Related Commands

Command	Description
protocol (L2TP)	Specifies the Layer 2 signaling protocol to be used to manage the pseudowires created from a pseudowire class for a dynamic Layer 2 session, and that control plane configuration settings are to be taken from the specified L2TP class
pseudowire	Binds an attachment circuit to a Layer 2 pseudowire for xconnect service.
pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

lapb interface-outage

To specify the period for which a link will remain connected, even if a brief hardware outage occurs (partial Link Access Procedure, Balanced [LAPB] T3 timer functionality), use the **lapb interface-outage** interface configuration command.

lapb interface-outage *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) a hardware outage can last without the protocol disconnecting the service.

Defaults

0 ms, which disables this feature.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If a hardware outage lasts longer than the LAPB hardware outage period you select, normal protocol operations will occur. The link will be declared down, and when it is restored, a link setup will be initiated.

Examples

The following example sets the interface outage period to 100 ms. The link remains connected for outages equal to or shorter than that period.

```
encapsulation lapb dte ip
lapb interface-outage 100
```

Related Commands

Command	Description
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb k

To specify the maximum permissible number of outstanding frames, called the *window size*, use the **lapb k** interface configuration command.

lapb k *window-size*

Syntax Description

window-size	Frame count. It can be a value from 1 to the modulo size minus 1 (the maximum is 7 if the modulo size is 8; it is 127 if the modulo size is 128).

Defaults

7 frames

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

If the window size is changed while the protocol is up, the new value takes effect only when the protocol is reset. You will be informed that the new value will not take effect immediately.

When using the Link Access Procedure, Balanced (LAPB) modulo 128 mode (extended mode), you must increase the window parameter k to send a larger number of frames before acknowledgment is required. This increase is the basis for the router's ability to achieve greater throughput on high-speed links that have a low error rate.

This configured value must match the value configured in the peer X.25 switch. Nonmatching values will cause repeated LAPB reject (REJ) frames.

Examples

The following example sets the LAPB window size (the k parameter) to 10 frames:

```
interface serial 0
 lapb modulo
 lapb k 10
```

Related Commands

Command	Description
lapb modulo	Specifies the LAPB basic (modulo 8) or extended (modulo 128) protocol mode.

lapb modulo

To specify the Link Access Procedure, Balanced (LAPB) basic (modulo 8) or extended (modulo 128) protocol mode, use the **lapb modulo** interface configuration command.

lapb modulo *modulus*

Syntax Description

modulus	Either 8 or 128. The value 8 specifies LAPB's basic mode; the value 128 specifies LAPB's extended mode.

Defaults

Modulo 8

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The modulo parameter determines which of LAPB's two modes is to be used. The modulo values derive from the fact that basic mode numbers information frames between 0 and 7, whereas extended mode numbers them between 0 and 127. Basic mode is widely available and is sufficient for most links. Extended mode is an optional LAPB feature that may achieve greater throughput on high-speed links that have a low error rate.

The LAPB operating mode may be set on X.25 links as well as LAPB links. The X.25 modulo is independent of the LAPB layer modulo. Both ends of a link must use the same LAPB mode.

When using modulo 128 mode, you must increase the window parameter k to send a larger number of frames before acknowledgment is required. This increase is the basis for the router's ability to achieve greater throughput on high-speed links that have a low error rate.

If the modulo value is changed while the protocol is up, the new value takes effect only when the protocol is reset. You will be informed that the new value will not take effect immediately.

Examples

The following example configures a high-speed X.25 link to use LAPB's extended mode:

```
interface serial 1
 encapsulation x25
 lapb modulo 128
 lapb k 40
 clock rate 2000000
```

Related Commands

Command	Description
lapb k	Specifies the maximum permissible number of outstanding frames, called the window size.

lapb n1

To specify the maximum number of bits a frame can hold (the Link Access Procedure, Balanced [LAPB] N1 parameter), use the **lapb n1** interface configuration command.

lapb n1 *bits*

Syntax Description

bits	Maximum number of bits in multiples of eight. The minimum and maximum range is dynamically set. Use the question mark (**?**) to view the range.

Defaults

The largest (maximum) value available for the particular interface is the default. The Cisco IOS software dynamically calculates N1 whenever you change the maximum transmission unit (MTU), the L2/L3 modulo, or compression on a LAPB interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The Cisco IOS software uses the following formula to determine the minimum N1 value:

*(128 (default packet size) + LAPB overhead + X.25 overhead + 2 bytes of CRC) * 8*

The Cisco IOS software uses the following formula to determine for the maximum N1 value:

*(hardware MTU + LAPB overhead + X.25 overhead + 2 bytes of CRC) * 8*

LAPB overhead is 2 bytes for modulo 8 and 3 bytes for modulo 128.

X.25 overhead is 3 bytes for modulo 8 and 4 bytes for modulo 128.

You need not set N1 to an exact value to support a particular X.25 data packet size. The N1 parameter prevents the processing of any huge frames that result from a "jabbering" interface, an unlikely event.

In addition, the various standards bodies specify that N1 be given in bits rather than bytes. While some equipment can be configured in bytes or will automatically adjust for some of the overhead information present, Cisco devices are configured using the true value, in bits, of N1.

You cannot set the N1 parameter to a value less than that required to support an X.25 data packet size of 128 bytes. All X.25 implementations must be able to support 128-byte data packets. Moreover, if you configure N1 to be less than 2104 bits, you receive a warning message that X.25 might have problems because some nondata packets can use up to 259 bytes.

You cannot set the N1 parameter to a value larger than the default unless the hardware MTU size is first increased.

The X.25 software accepts default packet sizes and calls that specify maximum packet sizes greater than those the LAPB layer supports, but negotiates the calls placed on the interface to the largest value that can be supported. For switched calls, the packet size negotiation takes place end-to-end through the router so the call will not have a maximum packet size that exceeds the capability of either of the two interfaces involved.

Caution The LAPB N1 parameter provides little benefit beyond the interface MTU and can easily cause link failures if misconfigured. Cisco recommends that this parameter be left at its default value.

Examples

The following example shows how to use the question mark (**?**) command to display the minimum and maximum N1 value. In this example, X.25 encapsulation has both the LAPB and X.25 modulo set to 8. Any violation of this N1 range results in an "Invalid input" error message.

```
router(config)# interface serial 1
router(config-if)# lapb n1 ?

<1080-12056> LAPB N1 parameter (bits; multiple of 8)
```

The following example sets the N1 bits to 16440:

```
router(config)# interface serial 0
router(config-if)# lapb n1 16440
router(config-if)# mtu 2048
```

Related Commands

Command	Description
lapb interface-outage	Partial LAPB T3 timer function that sets the time-length a link will remain connected during a hardware outage.
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.
mtu	Adjusts the maximum packet size or MTU size.

lapb n2

To specify the maximum number of times a data frame can be sent (the Link Access Procedure, Balanced [LAPB] N2 parameter), use the **lapb n2** interface configuration command.

lapb n2 *tries*

Syntax Description

tries	Transmission count. It can be a value from 1 to 255.

Defaults

20 transmissions

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example sets the N2 tries to 50:

```
interface serial 0
 lapb n2 50
```

Related Commands

Command	Description
lapb interface-outage	Partial LAPB T3 timer function that sets the time-length a link will remain connected during a hardware outage.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb protocol

The **lapb protocol** command has been replaced by the [*protocol* | **multi**] option of the **encapsulation lapb** command. See the description of the [*protocol* | **multi**] option of the **encapsulation lapb** command earlier in this chapter for more information.

lapb t1

To set the retransmission timer period (the Link Access Procedure, Balanced [LAPB] T1 parameter), use the **lapb t1** interface configuration command.

lapb t1 *milliseconds*

Syntax Description

milliseconds	Time in milliseconds. It can be a value from 1 to 64000.

Defaults

3000 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The retransmission timer determines how long a transmitted frame can remain unacknowledged before the LAPB software polls for an acknowledgment. The design of the LAPB protocol specifies that a frame is presumed to be lost if it is not acknowledged within T1; a T1 value that is too small may result in duplicated control information, which can severely disrupt service.

To determine an optimal value for the retransmission timer, use the **ping** privileged EXEC command to measure the round-trip time of a maximum-sized frame on the link. Multiply this time by a safety factor that takes into account the speed of the link, the link quality, and the distance. A typical safety factor is 1.5. Choosing a larger safety factor can result in slower data transfer if the line is noisy. However, this disadvantage is minor compared to the excessive retransmissions and effective bandwidth reduction caused by a timer setting that is too small.

Examples

The following example sets the T1 retransmission timer to 2000 ms:

```
interface serial 0
 lapb t1 2000
```

Related Commands

Command	Description
lapb interface-outage	Partial LAPB T3 timer function that sets the time-length a link will remain connected during a hardware outage.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).

Command	Description
lapb t2	Sets the explicit acknowledge deferral timer (LAPB T2 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb t2

To set the explicit acknowledge deferral timer (the Link Access Procedure, Balanced [LAPB] T2 parameter), use the **lapb t2** interface configuration command.

lapb t2 *milliseconds*

Syntax Description

milliseconds	Time in milliseconds. It can be a value from 1 to 32000. Default is 0 ms (disabled) and the recommended setting.

Defaults

0 ms (disabled), which means that the software will send an acknowledgement as quickly as possible.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

The explicit acknowledge deferral timer determines the time that the software waits before sending an explicit acknowledgement. The acknowledgement is piggybacked with the data, unless there is no data and then an explicit acknowledgement is sent when the timer expires.

Caution It is usually not necessary (or recommended) to set the LAPB T2 timer, but if there is a requirement, it must be set to a value smaller than that set for the LAPB T1 timer; see the ITU X.25 specifications for details.

Related Commands

Command	Description
lapb interface-outage	Partial LAPB T3 timer function that sets the time-length a link will remain connected during a hardware outage.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

lapb t4

To set the T4 idle timer, after which the Cisco IOS software sends out a Poll packet to determine whether the link has suffered an unsignaled failure, use the **lapb t4** interface configuration command.

lapb t4 *seconds*

Syntax Description

seconds	Number of seconds between receipt of the last frame and transmission of the outgoing poll.

Defaults

0 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Any non-zero T4 duration must be greater than T1, the Link Access Procedure, Balanced (LAPB) retransmission timer period.

Examples

The following example will poll the other end of an active link if it has been 10 seconds since the last frame was received. If the far host has failed, the service will be declared down after **n2** tries are timed out.

```
interface serial0
 encapsulation x25
 lapb t4 10
```

Related Commands

Command	Description
lapb interface-outage	Partial LAPB T3 timer function that sets the time-length a link will remain connected during a hardware outage.
lapb n1	Sets the maximum number of bits a frame can hold (LAPB N1 parameter).
lapb n2	Specifies the maximum number of times a data frame can be sent (LAPB N2 parameter).
lapb t1	Sets the retransmission timer period (LAPB T1 parameter).
lapb t4	Sets the LAPB T4 idle timer, after which time a poll packet is sent to determine state of an unsignaled failure on the link.

logging event frame-relay x25

To enable notification of X.25 Annex G session status changes to be displayed on a console or system log, use the **logging event frame-relay x25** command in interface configuration mode. To disable notification, use the **no** form of this command.

logging event frame-relay x25

no logging event frame-relay x25

Syntax Description

This command has no arguments or keywords.

Defaults

X.25 Annex G session status change notifications are not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Examples

The following example shows how to enable notification of X.25 Annex G session status changes to be displayed on a console or system log using the **logging event frame-relay x25** interface configuration command:

```
Router(config-if)# logging event frame-relay x25
```

The following is an example of the Annex G status change notifications:

```
%X25-5-UPDOWN: Interface <interface> - DLCI <dlci number> X.25 packet layer changed state
to DOWN
%X25-5-UPDOWN: Interface <interface> - DLCI <dlci number> X25 packet layer changed state
to UP
```

loopback

To loop packets back to the interface for testing, use the **loopback** interface configuration command with or without an optional keyword. To remove the loopback, use the **no** form of this command.

Cisco 2600 and 3600 Series

loopback [**line** | **local** | **payload** | **remote**]

no loopback [**line** | **local** | **payload** | **remote**]

Cisco 7100, 7200, and 7500 Series

For T1 lines:

loopback {**diagnostic** | **local** {**payload** | **line**} | **remote** {**iboc** | **esf** {**payload** | **line**}}}

For E1 lines:

loopback {**diagnostic** | **local** {**payload** | **line**}}

no loopback

Syntax Description

line	Places the interface into external loopback mode at the line.
local	Places the interface into local loopback mode.
payload	Places the interface into external loopback mode at the payload level.
remote	Keeps the local end of the connection in remote loopback mode.
diagnostic	Loops the outgoing transmit signal back to the receive signal.
iboc	Sends an in-band code to the far-end receiver to cause it to go into line loopback.
esf	Specifies the FDL loopbacks. FDL should be configured on the link.

Defaults

The **line** keyword is the default.
Loopback is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3 MA	This command was modified for the Cisco MC3810.
12.0(5)XK	Support for the Cisco 2600 and 3600 series routers was added.
12.0(5)T	Support for the Cisco 2600 and 3600 series routers was integrated into Cisco IOS Release 12.0(5)T.
12.0(5)XE	Support for the Cisco 720 0 and 7500 series routers was added.

Release	Modification
12.0(7)XE1	Support for the Cisco 7100 series routers was added.
12.1(5)T	Support for Cisco 7100, 7200, and 7500 series routers was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

You can use a loopback test on lines to detect and distinguish equipment malfunctions caused either by line and channel service unit/digital service unit (CSU/DSU) or by the interface. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem.

The local loopback does not generate any packets automatically. Instead, the **ping** command is used.

Examples

The following example sets up local loopback diagnostics:

```
interface atm 1/0
 loopback local
```

loopback (ATM)

To configure the ATM interface into loopback mode, use the **loopback** interface configuration command. To remove the loopback, use the **no** form of this command.

loopback [**cell** | **line** | **payload**]

no loopback [**cell** | **line** | **payload**]

Syntax Description

cell	(Optional) Places the interface into external loopback at cell level.
line	(Optional) Places the interface into external loopback at the line.
payload	(Optional) Places the interface into external loopback at the payload level.

Defaults

line

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
11.1	The following keywords were removed: • **diagnostic** • **test**

Usage Guidelines

This command is useful for testing because it loops all packets from the ATM interface back to the interface as well as directing the packets to the network.

Use the **loopback line** command to check that the PA-A3 port adapter is working by looping the receive data back to the transmit data.

Examples

The following example loops all packets back to the ATM interface:

```
interface atm 4/0
 loopback
```

Related Commands

Command	Description
ces dsx1 loopback	Enables a loopback for the CBR interface.