hello through lz entropy-check

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 between sending hello keepalive packets to its peer router. The valid values range from 0 to 1000 seconds. The default value is 60 seconds.

Command Default

The router sends hello keepalive packets at 60 second intervals.

Command Default

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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

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 (AV) pair values in Layer 2 Tunneling Protocol (L2TP) control messages, use the **hidden** command in L2TP class configuration mode. To unhide AV pairs, use the **no** form of this command.

hidden
no hidden

Syntax Description   This command has no arguments or keywords.

Command Default   L2TP AV pair 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(29)S	This command was modified to function only with the authentication method configured with the **digest secret** command and keyword combination.
12.2(27)SBC	This command was modified to function only with the authentication method configured with the **digest secret** command and keyword combination.

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.

In Cisco IOS Release 12.0(29)S and Cisco IOS Release 12.2(27)SBC, only the hiding of the cookie AVP is supported.

In Cisco IOS Release 12.0(29)S and Cisco IOS Release 12.2(27)SBC, this command was modified to function only with the authentication method configured using the **digest secret** command and keyword combination. AVP hiding is enabled only when both the **digest secret** command and keyword combination and the **hidden** command have been issued. If another method of authentication is also configured, such as Challenge Handshake Authentication Protocol (CHAP) style authentication configured with the L2TP class command **authentication**, AVP hiding will not be enabled.

If AVP hiding is configured, the session local cookie will be hidden when sent in incoming-call-request (ICRQ) and incoming-call-reply (ICRP) messages.

Whether or not AVP hiding is enabled, if a hidden AVP is received the AVP will be unhidden using the shared secret configured with the **digest secret** command and keyword combination. If no shared secret is configured, the AVP will not be unhidden and an error will be reported. If the M-bit is set in the received hidden AVP, the control channel or tunnel will be torn down.

Examples

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

```
Router(config)
# l2tp-class l2tp-class1
Router
(config-l2tp-class)
# digest secret cisco hash sha
Router(config-l2tp-class)
# hidden
```

Related Commands

Command	Description
digest	Enables L2TPv3 control channel authentication or integrity checking.
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 hostname 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 hostname, use the **no** form of this command.

hostname *name*
no hostname *name*

Syntax Description

name	Name used to identify the router during authentication.

Command Default

No hostname 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

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

Examples

The following example configures the hostname "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.

hostname dynamic (OTV)

To configure dynamic hostname exchange, use the **hostname dynamic** command in OTV IS-IS instance configuration mode. To remove the configuration, use the **no** form of this command.

hostname dynamic
no hostname dynamic

Syntax Description   This command has no arguments or keywords.

Command Default   Dynamic hostname exchange is enabled by default.

Command Modes   OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples   The following example shows how to configure dynamic hostname exchange:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# hostname dynamic
Router(config-otv-isis)# end
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

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.

Command Default   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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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 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** command in global configuration mode. 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.

Command Default 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.
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 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: 0 to 2147483647.

Command Default A Frame Relay bundle interface is not configured.

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.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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	This command was integrated into Cisco IOS XE Release.

Usage Guidelines Frame Relay encapsulation is the default encapsulation type for multilink Frame Relay bundle interfaces.

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 bandwidth-class	Specifies the bandwidth class used to trigger activation or deactivation of the Frame Relay 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 nve

To create a network virtualization endpoint (NVE) interface and enter NVE interface configuration mode, use the **interface nve** command in global configuration mode. To remove the NVE interface, use the **no** form of this command.

interface nve *number*
no interface nve *number*

Syntax Description	**number** The NVE interface number.

Command Default   No default.

Command Modes   Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced on the Cisco CSR 1000V.

Example

The following example enters NVE interface mode:

```
Router(config)# interface nve 1
Router(config-if)#
```

interface overlay

To create an Overlay Transport Virtualization (OTV) overlay interface, use the **interface overlay** command in global configuration mode. To remove the overlay interface, use the **no** form of this command.

interface overlay *interface*
no interface overlay *interface*

Syntax Description

| *interface* | Number that you assign to the overlay interface. The range is from 0 to 512. |

Command Default

The overlay interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

The **interface overlay** command creates a new overlay interface if none exists for the specified *interface* value. The specified *interface* value is locally significant only on the edge device. If you use the **no** form of the command, the specified overlay interface is deleted along with all other configurations done in this configuration mode.

You can also create an overlay interface by using the **otv isis overlay** command. An IS-IS overlay instance is automatically created when you use either the **interface overlay** command or the **otv isis overlay** command.

The **no interface overlay** command automatically removes the IS-IS overlay instance.

Examples

The following example shows how to create an OTV overlay interface:

```
Router# configure terminal
Router(config)# interface overlay 1
Router(config-if)# end
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV IS-IS instance.
show otv	Displays information about OTV.

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.

Command Default

This command has no default values.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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.

interworking

To enable Layer 2 VPN (L2VPN) interworking, use the **interworking** command in pseudowire class configuration or xconnect configuration mode. To disable L2VPN interworking, use the **no** form of this command.

interworking {**ethernet** | **ip** | **vlan**}
no **interworking** {**ethernet** | **ip** | **vlan**}

Syntax Description

ethernet	Causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. It is assumed that Ethernet has end-to-end transmission. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, which leaves a pure Ethernet frame.
ip	Causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. The attachment circuit frames that do not contain IPv4 packets are dropped.
vlan	Causes Ethernet frames and the VLAN tag to be sent over the pseudowire. It is assumed that Ethernet has end-to-end transmission. The attachment circuit frames that do not contain Ethernet frames are dropped.

Command Default   L2VPN interworking is disabled.

Command Modes   Pseudowire class configuration (config-pw-class)

Xconnect configuration (config-xconnect)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(52)SE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
12.2(33)SRE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
Cisco IOS XE Release 3.7S	This command was modified as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command was made available in xconnect configuration mode.

Usage Guidelines

The table below shows which L2VPN interworking features support Ethernet, IP, and VLAN types of interworking.

Table 1: L2VPN Interworking Feature Support

L2VPN Interworking Feature	Interworking Support
Frame Relay to PPP	IP
Frame Relay to ATM AAL5	IP
Ethernet/VLAN to ATM AAL5	IP and Ethernet
Ethernet/VLAN to Frame Relay	IP and Ethernet
Ethernet/VLAN to PPP	IP
Ethernet to VLAN	IP, Ethernet, and VLAN
L2VPN Interworking: VLAN Enable/Disable Option for AToM	Ethernet VLAN

Examples

The following example shows a pseudowire class configuration that enables the L2VPN interworking:

```
Device(config)# pseudowire-class ip-interworking
Device(config-pw-class)# encapsulation mpls
Device(config-pw-class)# interworking ip
```

The following example shows an xconnect configuration that enables L2VPN interworking:

```
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# interworking ip
```

Related Commands

Command	Description
encapsulation l2tpv3	Specifies that L2TPv3 is used as the data encapsulation method for tunneling IP traffic over the pseudowire.
encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.

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.

Command Default

On the Cisco 10720 Internet router and Cisco 12000 series Internet routers, the DF bit is on (enabled) by default. On other platforms, the DF bit is off (disabled) 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.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.0(32)SY	Support was added on the Cisco 10720 Internet router for the L2TPv3 Layer 2 fragmentation feature.

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 10720 Internet router and 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.

Command	Description
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.

Command Default No IP address is configured.

Command Modes

Pseudowire class configuration

Command History

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

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 the path maximum transmission unit (MTU) for Layer 2 traffic, use the **ip pmtu** command in VPDN group, VPDN template, 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. |

Command Default   Path MTU discovery is disabled.

Command Modes

VPDN group configuration (config-vpdn)
VPDN template configuration (config-vpdn-templ)
Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S and support was added for using this command in pseudowire class configuration mode.
12.3(2)T	Support was added for using this command in pseudowire class configuration mode.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Cisco IOS XE Release 2.6.2	This command was integrated into Cisco IOS XE Release 2.6.2.

Usage Guidelines   When the **ip pmtu** command is enabled, the Don't Fragment (DF) bit is copied from the inner IP header to the Layer 2 encapsulation header.

Enabling the **ip pmtu** command triggers Internet Control Message Protocol (ICMP) unreachable messages that indicate fragmentation errors in the IP backbone network carrying the tunneled traffic. If an IP packet is larger than the MTU of any interface, it must pass through and the DF bit is set, the packet is dropped and an ICMP unreachable message is returned. The ICMP unreachable message indicates the MTU of the interface that was unable to forward the packet without fragmentation. This information allows the source host to reduce the size of the packet before retransmission, allowing it to fit through that interface.

Note   When path MTU discovery (PMTUD) is enabled, VPDN deployments are vulnerable to Denial of Service (DoS) attacks that use crafted Internet Control Message Protocol (ICMP) "fragmentation needed and Don't Fragment (DF) bit set" (code 4) messages, also known as PMTUD attacks. Crafted code 4 ICMP messages can be used to set the path MTU to an impractically low value. This will cause higher layer protocols to time out because of a very low throughput, even though the connection is still in the established state. This type of attack is classified as a throughput-reduction attack. When PMTUD is enabled, it is highly recommended that you use the **vpdn pmtu** command to configure a range of acceptable values for the path MTU to block PMTUD attacks.

Enabling PMTUD will decrease switching performance.

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

When issued in VPDN template configuration mode, the **ip pmtu**command enables any tunnel associated with the specified VPDN template to participate in path MTU discovery.

When issued in pseudowire class configuration mode, the **ip pmtu**command enables any Layer 2 Tunnel Protocol Version 3 (L2TPv3) session derived from the specified pseudowire class configuration to participate in path MTU discovery.

Examples   The following example configures a VPDN group named dial-in on a Layer 2 Tunnel Protocol (L2TP) tunnel server and uses the **ip pmtu** command to specify that tunnels associated with this VPDN group will participate in path MTU discovery. The **vpdn pmtu** command is used to configure the device to accept only path MTU values ranging from 576 to 1460 bytes. The device will ignore code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)
# vpdn-group dial-in
Router(config-vpdn)
# request-dialin
Router(config-vpdn-acc-in)
# protocol l2tp
Router(config-vpdn-acc-in)
# virtual-template 1
!
Router(config-vpdn)
# l2tp security crypto-profile l2tp
Router(config-vpdn)
# no l2tp tunnel authentication
Router(config-vpdn)
# lcp renegotiation on-mismatch
Router(config-vpdn)
# ip pmtu
!
Router(config)
# vpdn pmtu maximum 1460
Router(config)
# vpdn pmtu minimum 576
```

The following example shows how to enable the discovery of the path MTU for pseudowires that are created from the pseudowire class named ether-pw. The **vpdn pmtu** command is used to configure the device to accept only path MTU values ranging from 576 to 1460 bytes. The device will ignore code 4 ICMP messages that specify a path MTU outside of this range.

```
Router(config)
# pseudowire-class ether-pw
Router(config-pw)
# ip pmtu
!
Router(config)
# vpdn pmtu maximum 1460
Router(config)
# vpdn pmtu minimum 576
```

Related Commands	**Command**	**Description**
	ip dfbit set	Enables the DF bit in the outer L2TPv3 tunnel header.
	ip mtu	Sets the MTU size of IP packets sent on an interface.
	ip mtu adjust	Enables automatic adjustment of the IP MTU on a virtual access interface.
	pseudowire-class	Specifies the name of an L2TP pseudowire class and enters pseudowire class configuration mode.
	vpdn pmtu	Manually configures a range of allowed path MTU sizes for an L2TP VPDN.
	vpdn-group	Creates a VPDN group and enters VPDN group configuration mode.
	vpdn-template	Creates a VPDN template and enters VPDN template 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.

Command Default   The default IP protocol is L2TP.

Command Modes

Pseudowire class configuration

Command History

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

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

Cisco ASR 901 Series Aggregation Services Routers
ip tos *value-number*

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.
value-number	ToS level for IP traffic in the pseudowire.

Command Default

The default ToS value is 0.

Command Modes

Pseudowire class configuration (config-pw-class)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

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:

```
Device(config)# pseudowire-class ether-pw
Device(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.

Command Default   The default value of the TTL byte is 255.

Command Modes   Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

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":

```
Device(config)# pseudowire-class ether-pw
Device(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** command in interface configuration mode. 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.

Command Default

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.2	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 **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 ke epalive 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.

l2 router-id

To specify a router ID for the provider edge (PE) router to use with Virtual Private LAN Services (VPLS) Autodiscovery pseudowires, use the l2 **router-id** command in L2 VFI configuration mode. To revert to the MPLS global router ID, use the **no** form of this command.

l2 router-id *ip-address*
no l2 router-id *ip-address*

Syntax Description

ip-address	Router ID in IP address format.

Command Default

The Layer 2 router ID is set to the Multiprotocol Label Switching (MPLS) global router ID.

Command Modes

L2 VFI configuration

Command History

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

Usage Guidelines

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

The Layer 2 router ID is used in the forward equivalence class (FEC) 129 encoding for pseudowire signaling It is also used in the network layer reachability information (NLRI) for peer discovery.

Examples

The following example specifies a Layer 2 router ID:

```
l2 router-id 10.1.1.1
```

Related Commands

Command	Description
l2 vfi autodiscovery	Enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.

l2 vfi autodiscovery

To enable the Virtual Private LAN Service (VPLS) provider edge (PE) router to automatically discover other PE routers that are part of the same VPLS domain, use the **l2 vfi autodiscovery** command in global configuration mode. To disable VPLS autodiscovery, use the **no** form of this command.

l2 vfi *vfi-name* **autodiscovery**
no l2 vfi *vfi-name* **autodiscovery**

Syntax Description

vfi-name	Specifies the name of the virtual forwarding instance. The virtual forwarding instance (VFI) identifies a group of pseudowires that are associated with a virtual switching instance (VSI).

Command Default

Layer 2 VFI autodiscovery is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

VPLS Autodiscovery enables each VPLS PE router to discover other PE routers that are part of the same VPLS domain. VPLS Autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain. Beginning with Cisco IOS Release 12.2(33)SRB, you no longer need to manually configure the VPLS neighbors and maintain the configuration when a PE router is added or deleted. However, you can still perform manual VPLS configuration even when you enable VPLS Autodiscovery.

Examples

The following example enables VPLS Autodiscovery on a PE router:

```
l2 vfi vfi2 autodiscovery
```

Related Commands

Command	Description
l2 vfi manual	Manually creates a Layer 2 VFI.

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.

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

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

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.

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

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

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.

Command Default

No hello keepalive messages are sent.

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

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 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.

Command	Description
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.
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.

Command Default

No session identifiers are configured.

Command Modes

Xconnect configuration (config-if-xconn)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

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 names 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, which can be inherited by different pseudowire classes, and to enter L2TP class configuration mode, use the **l2tp-class** command in global configuration mode. To remove a specific L2TP class configuration, use the **no**form of this command.

l2tp-class [*l2tp-class-name*]
no 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.

Command Default   No L2TP classes are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SCC	This command was integrated into Cisco IOS Release12.2(33)SCC.
12.2(50)SQ	This command was integrated into Cisco IOS Release 12.2(50)SQ.

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

- Hostname 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.

Note   For Cisco IOS Release 12.2(33)SCC and Cisco IOS Release 12.2(50)SQ, the commands listed under the Related Commands section are not valid.

Examples   The following example shows how to enter L2TP class configuration mode to create an L2TP class configuration template for a 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.

Command Default

0 ms, which disables this feature.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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. Range: 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).

Command Default

7 frames

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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.

Command Default

Modulo 8

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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.

Command Default

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.
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 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	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
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. Range: 1 to 255. |

Command Default

20 transmissions

Command Modes

Interface configuration

Command History

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

Examples

The following example sets the N2tries to 50:

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

Related Commands

Command	Description
lapb interface-outage	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
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. Range: 1 to 64000.

Command Default

3000 ms

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
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. Range: 1 to 32000. Default is 0 ms (disabled) and the recommended setting.

Command Default

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.
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 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	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
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.

Command Default 0 seconds

Command Modes

Interface configuration

Command History

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

Usage Guidelines 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	Sets the time-length a link will remain connected during a hardware outage by using a partial LAPB T3 timer function.
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.

log-adjacency-changes (OTV)

To configure the edge device to send a log message when the state of an IS-IS adjacency changes, use the **log-adjacency-changes** command in OTV IS-IS instance configuration mode. To disable sending the log message, use the **no** form of this command.

log-adjacency-changes [**all**]
no log-adjacency-changes

Syntax Description

all	(Optional) Specifies to include changes generated by a non-Intermediate System-to-Intermediate System Hello PDU (IIH) event.

Command Default

No log messages are sent when the state of an IS-IS neighbor changes.

Command Modes

OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following example shows how to configure an edge device to send a log message when there are changes in the adjacency state:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# log-adjacency-changes
Router(config-otv-isis)# end
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

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.

Command Default

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
```

lsp-gen-interval (OTV)

To configure a link-state packet (LSP) generation interval, use the **lsp-gen-interval** command in OTV IS-IS instance configuration mode. To remove the LSP generation interval configuration, use the **no** form of this command.

lsp-gen-interval *lsp-max-wait* [*lsp-initial-wait* *lsp-second-wait*]
no lsp-gen-interval

Syntax Description

lsp-max-wait	Interval in seconds. The range is from 1 to 120.
lsp-initial-wait	(Optional) Initial wait interval in milliseconds. The range is from 1 to 120000.
lsp-second-wait	(Optional) Interval in milliseconds between the first and second LSP generation. The range is from 1 to 120000.

Command Default

Layer 2 is configured, by default, with LSP generation intervals of 5 seconds, 50 milliseconds, and 200 milliseconds for the *lsp-max-wait*, *lsp-initial-wait*, and *lsp-second-wait* arguments, respectively.

Command Modes

OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

You can enter **lsp-gen-interval** commands by using different combinations of the arguments to control the rate of LSP packets being generated, transmitted, and retransmitted.

Examples

The following example shows how to configure an LSP generation interval:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# lsp-gen-interval 90 6000 7000
Router(config-otv-isis)# end
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

lsp-mtu (OTV)

To configure the link-state packet (LSP) maximum transmission unit (MTU), use the **lsp-mtu** command in OTV IS-IS instance configuration mode. To return to the default setting, use the **no** form of this command.

lsp-mtu *bytes*
no lsp-mtu

Syntax Description

bytes	Maximum LSP MTU size in bytes. The range is from 128 to 4352.

Command Default

The default Layer 2 LSP MTU is 1392 bytes.

Command Modes

OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following example shows how to set the maximum LSP size to 1500 bytes:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# lsp-mtu 1500
Router(config-otv-isis)# end
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

lsp-refresh-interval (OTV)

To configure a link-state packet (LSP) refresh interval in seconds, use the **lsp-refresh-interval** command in OTV IS-IS instance configuration mode. To remove the LSP refresh interval configuration, use the **no** form of this command.

lsp-refresh-interval *seconds*
no lsp-refresh-interval

Syntax Description

seconds	Refresh time interval in seconds. The range is from 1 to 65535.

Command Default

The default LSP refresh interval is 900 seconds (15 minutes).

Command Modes

OTV IS-IS instance configuration (config-otv-isis)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Examples

The following example shows how to configure the LSP refresh interval as 30 seconds:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# lsp-refresh-interval 30
Router(config-otv-isis)# end
```

Related Commands

Command	Description
otv isis overlay	Creates an OTV overlay interface.
show otv isis	Displays the IS-IS status and configuration.

lz entropy-check

To enable adaptive Lempel-Ziv (LZ) compression through entropy checking, use the **lz entropy-check** command in parameter-map configuration mode. To disable the LZ entropy checking, use the **no** form of this command.

lz entropy-check
no lz entropy-check

Syntax Description	This command has no arguments or keywords.
Command Default	Entropy checking is disabled.
Command Modes	Parameter-map configuration (config-profile)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines   Use this command to enable adaptive LZ compression through entropy checking.

Examples   The following example shows how to enable LZ entropy checking:

```
Router(config)# parameter-map type waas waas_global
Router(config-profile) lz entropy-check
```

Related Commands

Command	Description
cpu-threshold	Sets the CPU threshold limit.
parameter-map type waas	Defines a WAAS Express parameter map.
policy-map type waas	Configures WAAS Express policy map.
tfo auto-discovery blacklist	Configures the blocked list with autodiscovery for WAAS Express.
tfo optimize	Configures compression for WAAS Express.