ERICSSON

Configuring L2VPN

SYSTEM ADMINISTRATOR GUIDE

44/1543-CRA 119 1170/1-V1 Uen F

Contents

1 Overview

This document provides an overview of Layer 2 Virtual Private Networks (L2VPNs) and describes the tasks and commands used to configure, monitor, troubleshoot, and administer L2VPN features through the SmartEdge router.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

The following sections provide an overview of L2VPN.

1.1 L2VPN Implementation

For L2VPNs, customer edge (CE) routers send Layer 2 (L2) traffic to provider edge (PE) routers over L2 circuits configured between the PE and the CE routers. An L2 circuit can be any of the following:

- Ethernet port
- 802.1Q permanent virtual circuit (PVC)
- Frame Relay PVC
- Asynchronous Transfer Mode (ATM) PVC

Note: Do not configure an on-demand PVC as an attachment circuit in an L2VPN configuration.

An L2VPN is configured on PE routers. The purpose of an L2VPN configuration is to cross-connect a local L2 circuit with a corresponding remote L2 circuit through a label-switched path (LSP) tunnel that crosses the network backbone.

Figure 1 displays the network topology for an L2VPN configuration. The cross-connection between the local L2 circuit and the remote L2 circuit can be configured statically, or Label Distribution Protocol (LDP) can be used to discover the cross-connection between the local and remote L2 circuits.

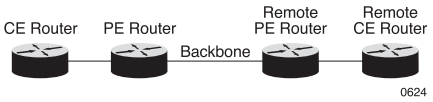

Figure 1 L2VPN Network Topology

L2VPN configuration is a three-step process:

1. Enable L2 circuits for L2VPN operation. An L2VPN is enabled on a context in context configuration mode. (Currently, an L2VPN can be enabled only on the local context).
2. Create an L2VPN cross-connection group. L2VPN cross-connection groups allow for convenient grouping of L2VPNs for display purposes; all L2VPNs configured within a cross-connection group are displayed together in the configuration.
3. Connect the L2VPN circuits within an L2VPN cross-connection group.

L2VPN configuration must be symmetric. That is, both PE routers (local and remote) must be configured using the same inner label (for a static L2VPN) or virtual circuit identifier (for a Label Distribution Protocol [LDP] L2VPN) and must also use the address of the remote PE as the peer address.

L2VPN supports circuit-to-pseudowire switching, where traffic reaching the PE is tunneled over a pseudowire (PW) (and, conversely, traffic arriving over the PW is sent out over the remote circuit). In this case, both ends of a PW are connected to circuits. Traffic received by the circuit is tunneled over the PW or, using local switching (also known as circuit-to-circuit cross-connect), the circuit switches packets or frames to another circuit attached to the same PE node.

Note: Static L2VPNs are not supported for ATM cell mode pseudowire cross-connections.

1.2 Supported Encapsulation Types

The SmartEdge router L2VPN implementation supports the following encapsulation types:

- Frame Relay Martini Encapsulation
- Ethernet VLAN
- Ethernet
- ATM (AAL5 and ATM cell mode)
- ATM RFC 1483 routed to Ethernet

1.2.1 Frame Relay Martini Encapsulation

Frame Relay Martini encapsulation is supported according to the Internet Draft, ***draft-martini-l2circuit-trans-mpls-10.txt***.

The Frame Relay virtual circuit (VC) type is always set to 0x0001. LDP sets the C-bit when establishing the VCs. When sending VC traffic to the core, a control word is attached to the packets, and Frame Relay data-link connection identifier (DLCI) information is stripped from the packets. The SmartEdge router uses preferred control word, as described in RFC 4385, *Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*. The egress PE router strips the control word from the packets and rebuilds the Frame Relay DLCI header before sending the traffic to the CE router.

The following considerations apply when configuring Frame Relay encapsulation:

- The VC type must be the same on both PE routers.
- The VC ID must be the same for both PE routers.
- The two CE routers can have different DLCIs because the Frame Relay DLCI information is stripped at ingress and rebuilt at egress.

1.2.2 Ethernet VLAN

Ethernet VLAN is supported in the raw mode with the Ethernet VLAN facility. With raw mode, no control word is sent with the traffic, and no C-bit is set. In raw mode, the whole VLAN header is sent to the remote PE router. On the egress side, the VLAN ID/tag is stripped and rebuilt according to the local VLAN tag.

The following considerations apply when configuring VLAN VCs:

- The VC type should be the same on both sides.
- The VC ID should be same for both sides for a VC.
- The two CE routers can have the same or different VLAN tags/permanent virtual circuits (PVCs) for the VC.

  Note: The SmartEdge router supports Ethernet VLAN tag stacking to support Extreme Networks switches' virtual metropolitan area network (VMAN) type of configuration. This configuration requires support for VLAN/VMAN tag 9100 in addition to the standard VLAN tag 8100. This support does not require any special L2VPN configuration on the SmartEdge router side. A sample configuration for this L2VPN environment is provided at the end of this section.

1.2.3 Ethernet

Ethernet implementation is the same as the Ethernet VLAN. Only raw mode is supported for Ethernet encapsulation.

1.2.4 ATM

The SmartEdge router supports two modes of ATM encapsulation:

- ATM adaptation layer 5 (AAL5) mode—Carries complete packets over the PW. In this ATM implementation, the AAL5 mode allows the transport of ATM AAL5 common part convergence sublayer-service data units (CPCS-SDUs) traveling on a particular ATM PVC across the network to another ATM PVC.
- ATM cell mode—Carries ATM cells over the PW from one ATM PVC across the network to another ATM PVC. In this mode, ATM cells are received and transmitted on the PVC without segmentation and reassembly (SAR).

The following considerations apply when configuring ATM VCs:

- The VC type should be the same on both sides of the VC.
- The VC ID should be the same on both sides.
- The ATM PVCs should be the same on both sides.

1.3 Supported Encapsulation Interconnectivity

TheSmartEdge router L2VPN implementation supports the following encapsulation types for interconnnectivity between two end-to-end cross-connections:

- ATM RFC 1483 bridged to Ethernet
- ATM RFC 1483 routed to Ethernet

Note: ATM RFC 1483 bridged to Ethernet is supported only if both end PE routers are SmartEdge 800 routers.

1.4 Pseudowire Cross-Connections

The SmartEdge router supports the following types of pseudowire cross-connections over MPLS networks:

- Ethernet-to-Ethernet
- ATM-to-ATM
- RFC 1483 bridged ATM-to-Ethernet
- 1483 routed ATM-to-Ethernet
- Frame Relay-to-Frame Relay
- VLAN-to-VLAN

The configuration of a pseudowire cross-connection is a four-step process:

1. Configure a connection between the local CE router and the local PE router.
2. Configure a pseudowire cross-connection endpoint on the local PE router.
3. Configure a connection between the remote CE router and the remote PE router.
4. Configure the remote pseudowire cross-connection endpoint on the remote PE router to bring up the pseudowire cross-connection. The local PE router and the remote PE router must share the same VC and pseudowire encapsulation type for the pseudowire cross-connection to be active.

The SmartEdge router supports pseudowire load balancing for L2VPN traffic. By default, load balancing is disabled and traffic from all channels of a pseudowire traverse the same path. When load balancing is enabled, traffic from individual channels in a pseudowire is distributed among the links in the link group. The load balancing scheme for each pseudowire is based on source and destination information. Use the **`pseudowire multi-path`** command in global configuration mode to enable load balancing on all L2VPN pseudowires configured on the router or in the current context. Be aware that load balancing is enabled and disabled in global configuration mode; this means that load balancing is globally enabled or disabled for all pseudowires that are configured on the router.

1.4.1 ATM-to-ATM Pseudowire Cross-Connections

The SmartEdge router supports the configuration of pseudowire cross-connections between two ATM circuits.

Figure 2 provides an example of a connection between two ATM circuits on two geographically dispersed CE routers. In this example, the local end of the pseudowire cross-connections is configured on an ATM circuit that connects to PE1, while the remote end of the pseudowire cross-connection is configured on an ATM circuit that connects to PE2.

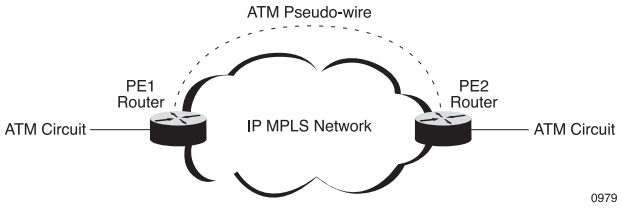

Figure 2 ATM-to-ATM Pseudowire Cross-Connections

Keep the following in mind when configuring an ATM-to-ATM pseudowire cross-connection:

- The SmartEdge router supports up to 16,000 PVCs per ATM card and 16,000 VCIs for each ATM card.

- ATM pseudowire cross-connections support ***n***-to-1 cell encapsulation on VCCs and VPCs, where ***n*** is equal to 1. To enable ***n***-to-1 cell encapsulation on an ATM pseudowire, use the **xc vc-id** command to configure the pseudowire type to be ***n***-to-1 VCC or ***n***-to-1 VPC.
- Cell mode encapsulation is supported only on ATM cards running in the default **vc-fair** mode. Cell mode-encapsulated PVCs cannot be provisioned if the ATM card is set to **atm-priority** mode or **ip-priority** mode. For more information about setting the ATM card mode with the **atm mode** command, see *Configuring Cards*.
- Cell concatenation is not supported on ATM pseudowire cross-connections.
- In VPC mode, you must configure an explicit range of VCIs for the ATM cells to be transported over the pseudowire cross-connection.
- ATM-to-ATM pseudowire cross-connections support the following encapsulation types:
  - AAL5
  - Cell mode

    Note: ATM cell mode encapsulation is not supported on SmartEdge 100 media interface cards (MICs).

1.4.1.1 Control Word

All pseudowire cross-connections allow you to enable or disable the inclusion of a control word in the cell header. The four-byte PW control word is inserted after the MPLS labels. The control word contains the following fields:

- 16-bit packet sequence number that is used to detect packet reordering and packet loss
- Payload length

  The sequence number is 16-bits and ranges from 1 through 65535. Sequence numbers are added to the control word in an incremental fashion, and the number wraps to 1 after reaching the maximum value. The inclusion of a sequence number ensures that packets are reordered properly if they become disassembled while traveling over the pseudowire. To enable the inclusion of a sequence number, enter the **control-word sequence-number**command in L2VPN XC group configuration mode. To disable the inclusion of a sequence number, enter the **control-word sequence-number 0** command.

  After you enable the inclusion of the control word, a single control word is included for each cross-connection group. The control word is applied to all pseudowires that are configured under the particular group.

  Be aware that, with ***n***-to-1 cell encapsulation, the control word is optional.

Note: For AAL5 encapsulated PWs, the control word is enabled by default.

1.4.2 1483 Routed ATM-to-Ethernet Pseudowire Cross-Connections

To support interconnectivity between the 1483 routed ATM and Ethernet protocols, you must configure an Ethernet pseudowire cross-connection between an ATM circuit and an Ethernet circuit on the PE routers. The Ethernet circuit can be pure Ethernet, or it can be a dot1q VLAN circuit.

Figure 3 provides an example of a connection between an ATM circuit and a VLAN circuit on two geographically dispersed CE routers. In this example, the local end of the pseudowire cross-connection is configured on an ATM circuit that is connected to PE1, while the remote end of the pseudowire cross-connection is configured on a dot1q VLAN port that connects to PE2.

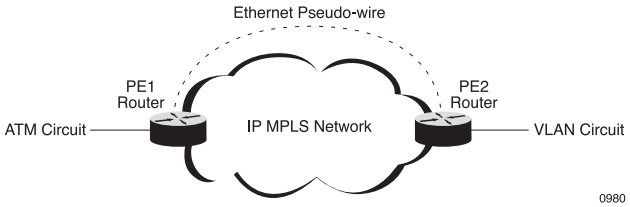

Figure 3 1483 Routed ATM-to-Ethernet Pseudowire Cross-connection

Keep the following in mind when configuring a 1483 routed ATM-to-VLAN cross-connection:

- The Ethernet pseudowire cross-connection supports both static and LDP-signaled configurations.
- VC multiplexing is not supported.

1.5 Ethernet Resiliency

The SmartEdge router supports Ethernet resiliency in L2VP configurations. Ethernet resiliency uses redundant Ethernet ports to provide resiliency. In a resilient Ethernet configuration, traffic destined for a particular circuit can be received on any of the constituent ports if the active Ethernet port goes down. The alternate port is automatically enabled to receive egress traffic. Alternate Ethernet port selection is automatic and cannot be administratively configured.

In L2VPN configurations, Ethernet resiliency is supported on the following types of cross-connections:

- Q-in-Q to Q-in-Q
- VLAN to Q-in-Q
- Q-in-Q to VLAN
- VLAN to VLAN

- Q-in-Q to ATM Bridged 1483
- VLAN to ATM Bridged 1483

In L2VPN configurations, traffic from the CE can be received on any of the constituent ports and is transported over the pseudowire cross-connection. All the traffic sent to the CE is sent over a particular constituent port that is selected by the SPG algorithm.

On the SmartEdge router, dot1q and Q-in-Q Ethernet circuits act as constituent ports when they are configured under an access link-group.

Traffic destined for an access link group circuit can be received by any of the constituent ports that are configured under the access link group circuit. Traffic is sent to the egress port as dictated by the cross-connect configuration. The SPG algorithm is used to pick an egress active port.

1.6 QoS Policies for L2VPN Circuits

Quality of Service (QoS) policies that are valid for L2VPN circuits can be applied to L2VPN attachment circuits. The following QoS policies can be applied to L2VPN circuits:

- Ingress rate limiting (policing) policies.
- Egress rate limiting (policing) policies.

  Note: Other types of QoS policies cannot be configured on L2VPN circuits.

In addition to supporting rate-limiting policing policies and metering type of shaping policies, L2VPN implementation also supports the following:

- L2VPN cross-connections with a Multiprotocol Label Switching (MPLS) experimental (EXP) bit configuration to forward traffic on certain backbone queues.
- dot1q profile configurations on L2VPN circuits to propagate dot1p bits to MPLS EXP bits, and MPLS EXP bits to dot1p bits.

For information about QoS policies, see *Configuring Rate-Limiting and Class-Limiting* and *Configuring Circuits for QoS*.

1.7 L2VPN over GRE

Encapsulating packets through Generic Routing Encapsulation (GRE) from an ingress PE router to an egress PE router is called soft GRE tunneling. Soft GRE tunnels are not Interior Gateway Protocol (IGP) visible links, and routing adjacencies are not supported across these tunnels. As a result, soft GRE

tunnels have little in common with traditional (hard) GRE tunnels. The tunnel exists only in the sense of GRE encapsulation and decapsulation.

Only the ingress PE router and the egress PE router need to support the soft GRE functionality, and the PE routers can span over multiple autonomous systems.

Using soft GRE tunnels to transport L2VPN-encapsulated packets is called L2VPN over GRE, and can be used instead of an MPLS tunnel in the backbone. L2VPN over GRE does not require preconfiguration of the remote GRE endpoint. The GRE tunnel endpoint is the address of the remote PE to which the L2VPN packets are being transported.

For more information about soft GRE, see *Configuring BGP/MPLS VPN*.

1.8 L2VPN XC-to-MPLS LSP Mapping

The SmartEdge router supports the mapping of an L2VPN XC to a specific MPLS LSP. The L2VPN XC-to-MPLS LSP mapping feature allows the system administrator to select a tunnel to carry traffic that is sent to a specific neighbor. Traffic can be mapped from an L2VPN XC to one of the following types of LSPs:

- RSVP
- LDP

If both RSVP and LDP LSPs are established between two PEs, you can map the XC to either an LDP LSP or an RSVP LSP. LDP LSPs use a lower configuration overhead than RSVP LSPs. You do not have to explicitly configure a particular LDP LSP; once an L2VPN XC is configured to map to an LDP LSP, that XC is automatically mapped to any LDP LSP that routes traffic to the PW destination.

By default, LSPs carry both PW and IP traffic. Such LSPs are considered non-exclusive. An LSP that carries only PW traffic is called an exclusive LSP. During LSP creation and configuration, you can use the **`exclusive`** command in RSVP LSP configuration mode to configure a mapped RSVP LSP to be exclusive. The advantage of an exclusive LSP is that it is only used for mapped traffic and is not shared. To configure an LSP to be exclusive, see the *Configure an RSVP LSP* section in *Configuring MPLS*.

Note: Only primary LSPs can be configured to be exclusive. Backup LSPs inherit exclusivity from the primary LSP.

If an XC is mapped to an LSP that has a backup or bypass LSP configured and the primary LSP goes down, the XC remains in the up state as long as the backup or bypass LSP is active. When a primary LSP goes down and it does not have a backup or bypass LSP configured, any XCs that are mapped to that LSP also go down.

1.9 L2VPN XC Redundancy

Note: L2VPN XC redundancy is supported for LDP signaled XCs only.

The SmartEdge router supports the ability to configure a standby L2VPN XC as a backup to a primary L2VPN XC. If the primary L2VPN XC fails, traffic fails over to the backup L2VPN XC.

By default, L2VPN XC redundancy is nonrevertive; in other words, traffic does not revert to the primary L2VPN XC when it becomes active again unless auto revert delay is enabled for the redundant XC pair. If you use the optional **`auto-revert-delay`** command in L2VPN profile peer configuration mode to enable auto-revert-delay on a pair of redundant XCs, the primary L2VPN XC becomes active again as soon as the auto-revert-delay timer runs out.

Note: When auto revert delay is not configured and a backup XC comes up before the primary XC, the backup XC remains active until a failure of the backup XC triggers a switchover to the primary XC.

The advantage of configuring L2VPN XC redundancy in your network is that it provides a redundant connectivity configuration that is used when an access circuit or access node fails. This feature enables your system to recover from failures on the remote PE router and active L2VPN XCs between the PE routers by switching to a backup L2VPN XC on an alternate PE.

You can also manually force a switch over from the active XC to the standby XC using the **`switchover pseudowire`** command in exec mode. See "L2VPN Operations."

L2VPN XC redundancy supports three modes of operation:

- Master-Slave mode—With this mode, Muley-signaling is enabled and the hub node serves as the master endpoint that selects which L2VPN XC to use for forwarding. The status of each active and standby L2VPN XC is communicated to the slave node through the signaling mechanism.
- Independent Redundancy mode—With this mode, Muley-signaling is enabled and the L2VPN XC endpoint nodes independently select which L2VPN XC is used for forwarding. Each node advertises its forwarding state over each L2VPN XC in a set. Each endpoint compares the local and remote status of its L2VPN XC and activates the L2VPN XC that is active at both endpoints.
- Default mode—With this mode, redundancy is not Muley-signaled, and the hub router that hosts the locally redundant pair of XCs selects which XCs act as the primary and backup. Traffic is forwarded over the active XC. Traffic that is received over the backup XC is dropped on the hub.

With the master-slave and independent redundancy modes, the SmartEdge router uses Muley-signaling to communicate the forwarding status of redundant XCs to their terminating points. Muley-signaling is described in the Internet draft document called *Pseudowire (PW) Redundancy*, draft-ietf-pwe-redundancy.txt.

With Muley-signaling, the forwarding standby status bit is used to select the active XC in a redundant pair. Use the **`redundancy-mode`** command to enable Muley-signaled L2VPN XC redundancy and select the redundancy operation mode for your system. If you do not use the **`redundancy-mode`** command to enable and configure Muley-signaled L2VPN XC redundancy operation, your system uses the default L2VPN XC mode, which is without Muley-signaled redundancy.

Consider the following rules and restrictions before configuring L2VPN XC redundancy on your SmartEdge router:

- L2VPN XC redundancy is supported on LDP-signaled L2VPN XCs only.
- Only one backup LVPN XC is support per primary L2VPN XC.
- For Muley-signaled L2VPN redundancy to work, both endpoints of the XC must support the PW status TLV. Be aware that on the SmartEdge router, the PWs support the PW status TLV by default.
- The backup L2VPN XC automatically inherits the experimental bits and the control word configuration from the primary L2VPN XC.
- A backup L2VPN XC can use the same VC ID as its primary XC if the active slave node is a different node than the standby slave node. If the active and slave nodes are configured on the same physical node (in different contexts), they cannot be configured with the same VC ID.
- In a hub-and-spoke networking using independent mode L2VPN XC redundancy, traffic that is forwarded from the spoke endpoints over a standby L2VPN XC is dropped at the hub PE because the spoke nodes do not have inter-chassis communication and always advertise an Active state to the hub node.

2 Configuration and Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command.

To configure an L2VPN, perform the tasks described in the following sections.

2.1 Enabling an L2 Circuit for L2VPN Operation

To enable an L2 circuit for L2VPN operation, perform the tasks described in Table 1.

Table 1 Enable an L2 Circuit for L2VPN Operation

Step	Task	Root Command	Notes
1.	Enable an ATM PVC for L2VPN operation.	*l2vpn (ctx-name)*	Enter this command in ATM PVC configuration mode.
2.	Enable an 802.1Q PVC for L2VPN operation.	*l2vpn (ctx-name)*	Enter this command in dot1q PVC configuration mode.
3.	Enable a Frame Relay PVC for L2VPN operation.	*l2vpn (ctx-name)*	Enter this command in Frame Rel configuration mode.
4.	Enable an Ethernet port for L2VPN operation.	*l2vpn (ctx-name)*	Enter this command in port config mode.

2.2 Enabling Load Balancing on Pseudowires

Use the **`pseudowire multi-path`** in global configuration mode to enable load balancing on all pseudowires (PWs) on the router. To disable load balancing on all pseudowires configured on the router, use the **`no pseudowire multi-path`** command in global configuration mode.

2.3 Configuring an LDP L2VPN Cross-Connection

To configure an LDP L2VPN cross-connection, perform the tasks described in Table 2.

Table 2 Configure an LDP L2VPN Cross-Connection

Step	Task	Root Command	Notes
1.	Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mod in a non-local context. L2VPN configuration is allowed only in the local context.
2.	Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.
3.	Create an LDP L2VPN cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. When creating a cross-connection to a remo circuit that uses an encapsulation type that different than the encapsulation type of the local circuit, use the **remote-encap** keywo to specify the encapsulation type used at th remote end of the cross-connection. The SmartEdge router supports the following encapsulation interconnectivity: • ATM RFC 1483 bridged to dot1q • ATM RFC 1483 bridged to Ethernet For ATM OC cards, you must specify a default channel number of 1 in the **xc vc-** command; for example, if the card is an ATM-OC3c/STM-1c, then you must specify default channel number of 1.
4.	Create an LDP L2VPN cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode.

2.4 Configuring a Static L2VPN Cross-Connection

To configure a static L2VPN cross-connection, perform the tasks described in Table 3.

Table 3 Configure a Static L2VPN Cross-Connection

Step	Task	Root Command	Notes
1.	Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configura mode. You cannot enter L2VPN configuration in a non-local context. L2VPN configura allowed only in the local context.
2.	Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configura mode.
3.	Create a static L2VPN cross-connection.	*xc (L2VPN vpn-label)*	Enter this command in L2VPN XC grou configuration mode. For ATM OC cards, you must specify de channel number of 1 in the **`xc vpn-la`** command; for example, if the card is a ATM-OC3c/STM-1c, then you must spe default channel number of 1.
4.	Create a static L2VPN cross-connection.	*xc (L2VPN vpn-label)*	Enter this command in L2VPN XC grou configuration mode.

2.5 Configuring a Cell Mode ATM-to-ATM Pseudowire Cross-Connection

You can configure a pseudowire cross-connection between two ATM circuits by configuring a single cell mode ATM PVC over a pseudowire cross-connection or by configuring a range of cell mode ATM PVCs over a single pseudowire cross-connection.

Before you can configure a pseudowire cross-connection between two ATM circuits on two geographically dispersed CE routers, you must perform the following tasks:

- Configure an ATM connection between a CE router and PE router that hosts one end of the pseudowire cross-connection.
- Configure a second ATM connection between a CE router and the PE router that hosts the other end of the pseudowire cross-connection.
- If you are configuring a range of PVCs, you must first create an ATM profile to apply to those PVCs, as described in *Configuring Circuits*.

See *Configuring ATM, Ethernet, and POS Ports* for information about configuring ATM connections.

Consider the following restrictions when configuring pseudowire cross-connection between two ATM circuits:

- The procedures in this section apply to cell mode-encapsulated ATM-to-ATM pseudowire cross-connections only.
- If you are configuring a range of PVCs, be aware that the control word applies only to the cell mode-encapsulated PVCs in the cross-connection group. The control word is not applied to PVCs that have AAL5 encapsulation.
- ATM cell mode encapsulation is not supported on the SmartEdge 100 media interface cards (MICs).
- For pseudowires carrying a single PVC, both ends of the PVC must share the same VPI.

2.5.1 Configure a Single Cell Mode ATM PVC over a Pseudowire Cross-Connection

To configure a single ATM PVC over a single pseudowire cross-connection, perform the tasks described in Table 4.

Table 4 Configure a Single Pseudowire Cross-Connection Between Two ATM Circuits

Task	Root Command	Notes
1. Configure the ATM circuit on the first PE router:		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Begin the configuration of the ATM port on the first PE router and access ATM OC configuration mode.	*port atm*	Enter this command in global configuration mode.
Create an ATM PVC and enter ATM PVC configuration mode.	*atm pvc*	Enter this command in ATM OC configuration mode. Use the **`encapsulation`** keyword to specify cell encapsulation. Use the **`profile`** keyword to specify an existing ATM profile.
Enable a Layer 2 (L2) circuit for Layer 2 Virtual Private Network (L2VPN) operation.	*l2vpn*	Enter this command in ATM PVC configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.

Table 4 Configure a Single Pseudowire Cross-Connection Between Two ATM Circuits

Task	Root Command	Notes
2. Configure one end of the pseudowire cross-connection on the first PE router. This router connects to the ATM CE router.		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Enter context configuration mode.	*context* **`local`**	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.
Optional. Specify that the control word is present in the pseudowire PDU and configure a sequence number increment or 0.	*control-word*	Enter this command in L2VPN XC group configuration mode. The control word is present on both PE routers that host the pseudowire cross-connection. If the negotiated value is set to yes, then only the control word is present in the PDU that is carried over the pseudowire. If you are configuring ***n***-to1 cell encapsulation on this pseudowire, then include the **`sequence-number 0`**keyword to disable the insertion of a control word.

Table 4 Configure a Single Pseudowire Cross-Connection Between Two ATM Circuits

Task	Root Command	Notes
Configure one endpoint of the L2VPN pseudowire cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same ***vpi/vci*** argument you specified for the ATM circuit with the **port atm** command. For ATM OC cards, you must specify a default channel number of 1 in the **xc vc-id** command; for example, if the card is an ATM-OC3c/STM-1c, then you must specify a default channel number of 1. Include the **cell-encap** keyword in the command to enable ATM cell-mode encapsulation on the cross-connection. Include the **nto1-vcc** keyword in the command to enable ***n***-to-1 VCC encapsulation. Include the **nto1-vpc** keyword in the command to configure ***n***-to-1 VPC encapsulation.
3. Configure the ATM circuit on the second PE router:		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Select an ATM port and enter port configuration mode.	*port atm*	Enter this command in global configuration mode.
Create an ATM PVC and enter ATM PVC configuration mode.	*atm pvc*	Enter this command in ATM OC configuration mode. Use the **profile** keyword to specify an existing ATM profile. Use the **encapsulation cell** keywords to specify cell encapsulation.
Enable the ATM circuit for L2VPN operation.	*l2vpn*	Enter this command in port configuration mode.
4. Configure the pseudowire cross-connection between the ATM circuits on the PE routers. Perform this configuration on the second router.		
Access global configuration mode.	*configure*	Enter this command in exec mode.

Table 4 Configure a Single Pseudowire Cross-Connection Between Two ATM Circuits

Task	Root Command	Notes
Enter context configuration mode.	*context* **local**	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.
Bring up the L2VPN cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same ***vpi/vci*** argument you specified for the first ATM circuit. Both endpoints of the pseudowire cross-connection must share the same VC ID for the connection to be active. Include the **cell-encap** keyword in the command to enable ATM cell-mode encapsulation on the cross-connection. Include the **nto1-vcc** keyword in the command to enable ***n***-to-1 VCC encapsulation. Include the **nto1-vpc** keyword in the command to configure ***n***-to-1 VPC encapsulation.

2.5.2 Configure a Range of Cell Mode ATM PVCs over a Single Pseudowire Cross-Connection

To configure a range of ATM PVCs over a single pseudowire cross-connection, perform the tasks described in Table 5.

Table 5 Configure a Range of PVCs over a Single Pseudowire Cross-Connection

Task	Root Command	Notes
1. Configure the ATM circuit on the first PE router:		

Table 5 Configure a Range of PVCs over a Single Pseudowire Cross-Connection

Task	Root Command	Notes
Access global configuration mode.	*configure*	Enter this command in exec mode.
Begin the configuration of an ATM port on the first PE router and access ATM OC configuration mode.	*port atm*	Enter this command in global configuration mode.
Create a range of static ATM PVCs and enter ATM PVC configuration mode.	*atm pvc* **explicit**	Enter this command in ATM OC configuration mode. Include the ***start-vpi:start-vci*** **through** ***end-vpi:end-vci*** constructs to specify the ranges of VCIs or VPIs. Include the **profile** ***prof-name*** construct to specify an existing ATM profile. Use the **encapsulation** keyword to specify cell encapsulation. Use the **profile** keyword to specify an existing ATM profile. Include the **n-to1** keyword in the command.
Enable a Layer 2 (L2) circuit for Layer 2 Virtual Private Network (L2VPN) operation.	*l2vpn*	Enter this command in ATM PVC configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.
2. Configure one end of the pseudowire cross-connection on the first PE router. This router connects to the ATM CE router.		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Enter context configuration mode.	*context* **local**	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.

Table 5 Configure a Range of PVCs over a Single Pseudowire Cross-Connection

Task	Root Command	Notes
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.
Configure one endpoint of the L2VPN pseudowire cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same ***vpi/vci*** argument you specified for the ATM circuit with the **port atm** command. For ATM OC cards, you must specify a default channel number of 1 in the **xc vc-id** command; for example, if the card is an ATM-OC3c/STM-1c, then you must specify a default channel number of 1. Include the **cell-encap** keyword in the command to enable ATM cell-mode encapsulation on the cross-connection. Include the **nto1-vcc** keyword in the command to enable ***n***-to-1 VCC encapsulation. Include the **nto1-vpc** keyword in the command to configure ***n***-to-1 VPC encapsulation.
3. Configure the ATM circuit on the second PE router:		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Select an ATM port and enter port configuration mode.	*port atm*	Enter this command in global configuration mode.

Table 5 Configure a Range of PVCs over a Single Pseudowire Cross-Connection

Task	Root Command	Notes
Create an ATM PVC and enter ATM PVC configuration mode.	*atm pvc* **explici t**	Enter this command in ATM OC configuration mode. Include the ***start-vpi:start-vci*th rough*end-vpi:end-vci*** constructs to specify the ranges of VCIs or VPIs. Include the **profile** ***prof-name*** keyword argument to specify an existing ATM profile. Use the **encapsulation** keyword to specify cell encapsulation. Use the **profile** keyword to specify an existing ATM profile. Include the **n-to1** keyword in the command.
Enable the ATM circuit for L2VPN operation.	*l2vpn*	Enter this command in port configuration mode.
4. Configure the pseudowire cross-connection between the ATM circuits on the PE routers. Perform this configuration on the second router.		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Enter context configuration mode.	*context* **local**	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.

Table 5 Configure a Range of PVCs over a Single Pseudowire Cross-Connection

Task	Root Command	Notes
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.
Bring up the L2VPN cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same ***vpi/vci*** argument you specified for the first ATM circuit. Include the **cell-encap** keyword in the command to enable ATM cell-mode encapsulation on the cross-connection. Include the **nto1-vcc** keyword in the command to enable ***n***-to-1 VCC encapsulation. Include the **nto1-vpc** keyword in the command to configure ***n***-to-1 VPC encapsulation. Both endpoints of the pseudowire cross-connection must share the same VC ID for the connection to be active.

2.6 Configuring a 1483 Routed ATM-to-Ethernet Pseudowire Cross-Connection

Use one of the following procedures described in this section to configure a pseudowire cross-connection between a 1483 routed ATM circuit and an Ethernet circuit.

Before you can configure a pseudowire cross-connection between a 1483 routed ATM circuit and an Ethernet circuit on two geographically dispersed CE routers, you must perform the following tasks:

- Configure an ATM connection between a CE router and PE router that hosts one end of the pseudowire cross-connection.
- Configure an Ethernet connection between a CE router and the PE router that hosts the other end of the pseudowire cross-connection

See *Configuring ATM, Ethernet, and POS Ports* for information about configuring ATM, Ethernet, and VLAN connections.

Note: 1483 routed ATM-to-Ethernet pseudowires support IPv4 frames only.

2.6.1 Configure a Pseudowire Between a 1483 Routed ATM Circuit and an Ethernet Circuit

To configure an Ethernet pseudowire cross-connection between a 1483 routed ATM circuit and an Ethernet circuit, perform the tasks described in Table 6.

Table 6 Configure an Ethernet Pseudowire Cross-Connection Between a 1483 Routed ATM Circuit and an Ethernet Circuit

Task	Root Command	Notes
1. Configure the ATM circuit on the first PE router:		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Begin the configuration of an ATM port on the first PE router and access ATM OC configuration mode.	*port atm*	Enter this command in global configuration mode.
Create an ATM PVC and enter ATM PVC configuration mode.	*atm PVC*	Enter this command in ATM OC configuration mode. Use the **`encapsulation`** keyword to specify routed 1483 encapsulation. Use the **`profile`** keyword to specify an existing ATM profile.
Enable a Layer 2 (L2) circuit for Layer 2 Virtual Private Network (L2VPN) operation.	*l2vpn*	Enter this command in ATM PVC configuration mode.
2. Configure one end of the pseudowire cross-connection on the first PE router. This router connects to the ATM CE router.		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Enter context configuration mode.	*context* **`local`**	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.

Table 6 Configure an Ethernet Pseudowire Cross-Connection Between a 1483 Routed ATM Circuit and an Ethernet Circuit

Task	Root Command	Notes
Configure one endpoint of the L2VPN pseudowire cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same ***vpi/vci*** argument you specified for the ATM circuit with the **port atm** command. Use the **remote-encap** keyword to specify the encapsulation type used at the remote end of the cross-connection. In this case, the remote end of the connection is **Ethernet**. For ATM OC cards, you must specify a default channel number of 1 in the **xc vc-id** command; for example, if the card is an ATM-OC3c/STM-1c, then you must specify a default channel number of 1. Include the **cell-encap** keyword in the command to enable ATM cell-mode encapsulation on the cross-connection. Include the **nto1-vcc** keyword in the command to enable ***n***-to-1 VCC encapsulation. Include the **nto1-vpc** keyword in the command to configure ***n***-to-1 VPC encapsulation.
3. Configure the Ethernet circuit on the second PE router:		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Select an Ethernet port and enter port configuration mode.	*port ethernet*	Enter this command in global configuration mode.
Enable a Layer 2 (L2) circuit for L2VPN operation.	*l2vpn*	Enter this command in port configuration mode.
4. Configure the pseudowire cross-connection between the VLAN circuit and the ATM circuit. Perform this configuration on the second router (the router that connects to the VLAN CE router).		
Access global configuration mode.	*configure*	Enter this command in exec mode.

Table 6 Configure an Ethernet Pseudowire Cross-Connection Between a 1483 Routed ATM Circuit and an Ethernet Circuit

Task	Root Command	Notes
Enter context configuration mode.	*context* `local`	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.
Bring up the L2VPN cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same Ethernet ***`slot`***`/`***`port`*** argument you configured on the second PE router. Both endpoints of the pseudowire cross-connection must share the same VC ID for the connection to be active.

2.6.2 Configure a Pseudowire Between a 1483 Routed ATM Circuit and a dot1Q VLAN Circuit

To configure an Ethernet pseudowire cross-connection between a 1483 routed ATM circuit and a VLAN, perform the tasks described in Table 7.

Table 7 Configure an Ethernet PW Cross-Connection Between a 1483 Routed ATM Circuit and a VLAN

Task	Root Command	Notes
1. Configure the ATM circuit on the first PE router:		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Begin the configuration of an ATM port on the first PE router, and access ATM OC configuration mode.	*port atm*	Enter this command in global configuration mode.

Table 7 Configure an Ethernet PW Cross-Connection Between a 1483 Routed ATM Circuit and a VLAN

Task	Root Command	Notes
Create an ATM PVC and enter ATM PVC configuration mode.	*atm PVC*	Enter this command in ATM OC configuration mode. Use the **`encapsulation`** keyword to specify routed 1483 encapsulation. Use the **`profile`** keyword to specify an existing ATM profile.
Enable a Layer 2 (L2) circuit for Layer 2 Virtual Private Network (L2VPN) operation.	*l2vpn*	Enter this command in ATM PVC configuration mode.
2. Configure one end of the pseudowire cross-connection on the first PE router. This router connects to the ATM CE router.		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Enter context configuration mode.	*context* **`local`**	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.

Table 7 Configure an Ethernet PW Cross-Connection Between a 1483 Routed ATM Circuit and a VLAN

Task	Root Command	Notes
Configure one endpoint of the L2VPN pseudowire cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same ***vpi/vci*** argument you specified for the ATM circuit with the **`port atm`** command. Use the **`remote-encap`** keyword to specify the encapsulation type used at the remote end of the cross-connection. In this case, the remote end of the connection is **`Ethernet`**. For ATM OC cards, you must specify a default channel number of 1 in the **`xc vc-id`** command; for example, if the card is an ATM-OC3c/STM-1c, then you must specify a default channel number of 1.
3. Configure the VLAN circuit on the second PE router:		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Select an Ethernet port and enter port configuration mode.	*port ethernet*	Enter this command in global configuration mode.
Specify the encapsulation for an Ethernet port to create 802.1Q permanent virtual circuits (PVCs).	*encapsulation*	Enter this command in port configuration mode. Use the **`dot1q`** keyword to specify 802.1Q encapsulation.
Create an 802.1Q PVC and access dot1q PVC configuration mode.	*dot1q pvc*	Enter this command in port configuration mode.
Enable a Layer 2 (L2) circuit for L2VPN operation.	*l2vpn*	Enter this command in port configuration mode.
4. Configure the pseudowire cross-connection between the VLAN circuit and the ATM circuit. Perform this configuration on the second router (the router that connects to the VLAN CE router).		
Access global configuration mode.	*configure*	Enter this command in exec mode.
Enter context configuration mode.	*context* **`local`**	Enter this command in global configuration mode.

Table 7 Configure an Ethernet PW Cross-Connection Between a 1483 Routed ATM Circuit and a VLAN

Task	Root Command	Notes
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode. You cannot enter L2VPN configuration mode in a nonlocal context. L2VPN configuration is allowed only in the local context.
Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group (L2VPN)*	Enter this command in L2VPN configuration mode.
Bring up the L2VPN cross-connection.	*xc (L2VPN vc-id)*	Enter this command in L2VPN XC group configuration mode. Use the same Ethernet ***slot*/*port*** argument you configured on the second PE router. Both endpoints of the pseudowire cross-connection must share the same VC ID for the connection to be active.

2.7 Enabling Soft GRE Tunneling

To enable soft GRE tunneling, perform the tasks described in Table 8.

Table 8 Enable Soft GRE Tunneling

Task	Root Command	Notes
Enable soft GRE tunneling on the specified context.	*ip soft-gre*	Enter this command in context configuration mode. Using soft GRE tunnels to transport L2VPN-encapsulated packets is called L2VPN over GRE, and can be used instead of an MPLS tunnel in the backbone. L2VPN over GRE does not require preconfiguration of the remote GRE endpoint. The GRE tunnel endpoint is the remote PE router address to which the L2VPN packets are being transported.

2.8 Mapping L2VPN XCs to MPLS LSPs

This section describes how to map an L2VPN XC to an MPLS LSP. The mapping of L2VPN XCs to an MPLS LSP comprises the following two steps:

- Create an L2VPN profile that specifies the LDP LSP or LSP tunnel to be mapped to an XC, and sets additional XC attributes, as described in Create an L2VPN Profile.
- Use the **xc** command to attach the L2VPN profile to the XC you want to map, as described in the Associate an L2VPN Profile in an XC Configuration section. The attributes in the L2VPN profile are automatically applied to the XC to which the profile is attached.

Consider the following restrictions before enabling mapping from an XC to an MPLS tunnel:

- If an L2VPN XC is mapped to an LSP that does not have a backup LSP configured, then the XC transitions to a down state if the primary LSP goes down.
- If an L2VPN XC is mapped to an LSP that is not protected by Fast Reroute, then the L2VPN XC transitions to a down state if the LSP goes down.
- An L2VPN XC that is mapped to an RSVP LSP must resolve on the same RSVP LSP.
- An L2VPN XC that is mapped to an LDP LSP must resolve on an LDP LSP. In this case, the XC can resolve on any LDP LSP that routes traffic to the PW destination.
- When an LDP LSP is not configured as the best path, only mapped PW traffic can flow on that LDP LSP.
- When an LDP LSP is configured as the best path, it supports both PW and unmapped traffic.
- When non-exclusive RSVP LSPs are available for a given IP destination, those LSPs carry both L2VPN and IP traffic.
- If all available RSVP LSPs are configured to be exclusive and an LDP LSP is available, then that LDP LSP path is used for both L2VPN and IP traffic.
- If all RSVP LSPs are configured to be exclusive, and there are no LDP LSPs available, then unmapped L2VPN XCs do not come up, and the unmapped L2VPN XCs that are already up transition to a down state.
- If all of the available RSVP LSPs are marked as exclusive, and no LDP LSPs are available for a given IP destination, then no LSP paths are available for L2VPN and native IP traffic, and that traffic is dropped.

2.8.1 Create an L2VPN Profile

Before you can map an XC to an LSP, you need to create an L2VPN profile that specifies the LDP LSP or RSVP LSP tunnel to be mapped to an XC, and sets additional XC attributes. To create an L2VPN profile, perform the tasks described in Table 9.

Table 9 Create an L2VPN Profile

#	Task	Root Command	Notes
1.	Enter global configuration mode.	*configure*	—
2.	Create an L2VPN profile, and enter L2VPN profile configuration mode.	*l2vpn profile* ***profile-name***	Replace the profile-name argument with a name that identifies this L2VPN profile.
3.	Specify the IP address of the peer router that can be reached through the LSPs on the current router, and enter L2VPN profile peer configuration mode.	*peer* ***peer-addr***	Replace the peer-addr argument with the IP address of the peer router.
4.	Optional. Specify an LDP path or a specific LSP tunnel.	*tunnel* ***ldp-path*** or *tunnel lsp* ***lsp-name***	Enter the tunnel lsp ***tunnel-name*** command to specify a specific RSVP tunnel for carrying traffic exiting the VPLS. Replace the tunnel-name argument with the name of the RSVP tunnel on which to carry traffic exiting a VPLS. Enter the tunnel ldp-path command to map the L2VPN circuit to an LDP LSP.(1)
5.	Optional. Enable ATM cell mode encapsulation on the specified pseudowire cross-connection.	*cell-encap* {**nto1-vcc** | **nto1-vpc**}	Select **nto1-vcc**cell mode encapsulation or nto1-vpc cell mode encapsulation.(2)
6.	Optional. Enable the inclusion of a control word in the packet header and enables or disables the inclusion of incremental sequence numbers that ensure disassembled packets are reassembled properly.	*control-word* [**sequence-number** [**zero**]]	Include the optional **sequence-number** keyword to enable sequencing support on all packets. Include the optional zero keyword to disable sequencing support on all packets

Table 9 Create an L2VPN Profile

#	Task	Root Command	Notes
7.	Optional. Specify the encapsulation type used at the remote end of the cross-connection.	*remote encap* {**1qtunnel** | **bridge1483** | **dot1q** | **ethernet**}	Include one of the following keywords to specify the appropriate encapsulation type: • **1qtunnel**—Specifies 802.1Q tunnel (Q-in-Q) encapsulation. • **bridge1483**—Specifies ATM RFC 1483 bridged encapsulation. • **dot1q**—Specifies 802.1Q Ethernet encapsulation. • **ethernet**—Specifies Ethernet encapsulation.
8.	Optional. Specify the EXP bits to be used for transport.	*exp-bits* ***bits-num***	Replace the ***bits-num*** argument with the number of EXP bits to be used for transport. Range is from 0 to 7.
9.	Reference the L2VPN profile you created in the xc command string for the XCs you want to map.	To reference the L2VPN profile in the **xc** command string, see Table 10.	—

(1) Only one LSP configuration is allowed in a single L2VPN profile.
*(2) The **cell-encap** command is available for ATM PWs only.*

2.8.2 Associate an L2VPN Profile in an XC Configuration

To map traffic from a PW carrying traffic from a given XC to a specific RSVP tunnel, use the **xc** command to reference an L2VPN profile in the configuration for the XCs you want to map. To reference the L2VPN profile you created in Table 10 in an XC configuration, perform the tasks described in Table 10.

Table 10 Reference the L2VPN Profile in the XC command

#	Task	Root Command	Notes
1.	Enter global configuration mode.	*configure*	—
2.	Enter context configuration mode.	*context* ***ctx-name***	Replace the ***ctx-name*** argument with the name of the context that hosts the XCs you want to map(1)
3.	Enter L2VPN configuration mode.	*l2vpn*	—

Table 10 Reference the L2VPN Profile in the XC command

#	Task	Root Command	Notes
4.	Create a new L2VPN XC group and enter L2VPN XC group configuration mode for that group, or enter L2VPN XC group configuration mode for an existing L2VPN group.	*xc-group* {***group-name*** | **default**}	Replace the group-name argument with the name of the L2VPN cross-connection group that contains the XCs you want to map to, or enter the default keyword to configure the default L2VPN cross-connection group The L2VPN XC group contains the XCs you want to map.
5.	Reference the L2VPN profile in the XC command to map the LSP to the XC.	***xc*** {lg ***group_name***| ***slot/port*** [:***chan-num***] [:***sub-chan-num***]} **vc-id** ***vc-id*** <***options***> **profile** ***profile-name***	The following syntax is required: • Use the lg ***group_name*** to specify the access link group for the cross-connection, or use the ***slot/port***[:***chan-num***] [:***sub-chan-num***} string to specify an interface for the cross-connection. • Use the **vc-id** ***vc-id*** construct to specify the Virtual circuit (VC) identifier associated with the cross-connection. • Use the **profile** ***profile-name*** construct to associate an L2VPN profile to an XC. When you attach an L2VPN profile to an XC, the LSP that is specified in the profile is automatically mapped to the XC you are configuring. To see the other optional parameters that can be configured in the *xc* command, see the command reference page for the *xc* command.
6.	Create additional new mapped XCs, or map existing XCs to an LSP.	Repeat Steps 1 through 5.	—
7.	Verify your XC L2VPN configuration.	*show xc l2vpn*	—

(1) The XC configuration is supported in the local context only.

2.9 Configuring L2VPN XC Redundancy

To configure L2VPN XC on your router, perform the tasks in the following sections:

2.9.1 Configuring an L2VPN Profile for L2VPN XC Redundancy

To create and configure an L2VPN profile for L2VPN XC redundancy, perform the tasks described in Table 11.

Table 11 Configure an L2VPN Profile for L2VPN XC Redundancy

Task	Root Command	Notes
Enter global configuration mode.	*configure*	—
Create an L2VPN profile and enter L2VPN profile configuration mode, or enter L2VPN profile configuration mode for an existing L2VPN profile.	*l2vpn profile* **`profile-name`**	Replace the profile-name argument with a name that identifies this L2VPN profile.
Specify the IP address of the peer router that can be reached through the LSPs on the current router, and enter L2VPN profile peer configuration mode.	*peer* **`peer-addr`**	Replace the peer-addr argument with the IP address of the peer router that will host the remote end of the primary XC you are configuring.
Optional. Enable Muley-signaled L2VPN XC redundancy.	*redundancy-mode* {**`master-slave`** | **`independent`**}	Include the **`master-slave`** keyword to enable master-slave redundancy mode, or the **`independent`** keyword to enable independent mode.(1)
Optional. Enable auto revert on a redundant pair of LVPN XCs and sets the auto-revert timer for L2VPN XC redundancy.	*auto-revert-delay* **`seconds`**	Replace the **`seconds`** argument with the number of seconds that must pass before the SmartEdge router switches from the backup XC to a primary XC when both XCs become active.
Optional. Logs the state of any XCs that have this L2VPN profile attached.	*log-pw-up-down*	A log is created each time an XC transitions to the down, up, and standby states. The logs are saved in the syslog file or in a user-specified log file.

Table 11 Configure an L2VPN Profile for L2VPN XC Redundancy

Task	Root Command	Notes
Optional. Maps any L2VPN XCs that have this profile attached to an LDP LSP or and RSVP tunnel.	*tunnel* **`ldp-path`** or *tunnel lsp* **`lsp-name`**	All L2VPN circuits attached to this profile are mapped to an RSVP or LDP LSP. If you are mapping the XC to an RSVP tunnel, replace the **`lsp-name`** argument with the name of an RSVP tunnel to host the backup L2VPN XC.
Optional. Enable SNMP trap notifications per L2VPN profile.	*snmp trap*	Enables trap notifications for cross-connect state change events.
Configure other optional parameters.	For details on other options that can be specified in an L2VPN profile, see Create an L2VPN Profile.	—
Exit L2VPN profile peer configuration mode and enters L2VPN profile configuration mode.	*exit*	—
Optional. Specify the remote end of the backup L2VPN XC in a redundant pair, and enter L2VPN profile backup peer configuration mode.	*backup peer* **`peer-address`**	Replace the **`peer-address`** argument with the IP address of the peer that hosts the remote end of the backup L2VPN XC.
Optional. Maps any backup L2VPN XCs that have this profile attached to an LDP LSP or and RSVP tunnel.	*tunnel* **`ldp-path`** or *tunnel lsp* **`lsp-name`**	All L2VPN circuits attached to this profile are mapped to an RSVP or LDP LSP. If you are mapping the XC to an RSVP tunnel, replace the **`lsp-name`** argument with the name of an RSVP tunnel to host the backup L2VPN XC.

(1) If you do not enable Muley-signaled L2VPN XC redundancy, the XC use the default mode, where redundancy is not Muley-signaled, and the hub router that hosts the redundant pair of XCs selects which XCs act as the primary and backup.

2.9.2 Configuring the Redundant L2VPN XCs

To configure a redundant pair of L2VPN XCs, perform the tasks described in Table 12. Keep the following rules in mind when configuring the redundant XCs:

- You need to attach an L2VPN profile to the primary and backup XCs.

- Perform Step 1 through Step 3 on the local and remote endpoints of the primary and backup XCs in a redundant pair.
- The VC ID on the remote XC endpoint must match the VC ID you configured on local XC endpoint.

Table 12 Configure a Redundant Pair of L2VPN XCs

#	Task	Root Command	Notes
1.	Create an L2VPN cross-connection group and enter L2VPN XC group configuration mode.	*xc-group*	Enter this command in L2VPN configuration mode.
2.	Configure the endpoint of the XC, and enter primary L2VPN XC configuration mode	***xc*** {***slot/port*** [***options***] | **lg** ***link-group***} [***circuit-id***] **vc-id** ***vc-id*** <***options***> **profile*profile-name*** **backup**	Enter this command in L2VPN XC group configuration mode. Replace the ***vc-id*** argument with the VC identifier you want to associate with the primary XC. Replace the ***profile-name*** argument with the name of the profile you created or configured in Configuring an L2VPN Profile for L2VPN XC Redundancy. For a detailed description of additional options you can set with the **xc vc-id** command, see the *xc (L2VPN vc-id)* command page.
3.	Configure the VC ID and peer address for the backup XC and enter primary L2VPN XC configuration mode.	*vc-id* ***vc-id*** **peer** ***peer-address***	Replace the vc-id argument with the VC identifier you want to associate with the primary XC. Replace the ***peer-address*** argument this the IP address of the peer that hosts the remote end of this backup XC.
4.	Verify your primary and backup L2VPN XC configuration.	*show xc l2vpn*	—

2.10 L2VPN Operations

To manage L2VPN functions, perform the appropriate tasks described in Table 13. Enter the **`switchover pseudowire`** command in exec mode. Enter the **`show`** commands in any mode.

Table 13 L2VPN Operations Tasks

Task	**Root Command**
In a redundant Layer 2 VPN (L2VPN) cross-connection, force a switch over from the active XC to the standby XC.	*switchover pseudowire*
Enable the generation of debug messages for L2VPN events	*debug l2vpn*
Display the L2VPN-related configuration information.	*show configuration l2vpn*
Display L2VPN-related information for LDP L2VPN cross-connections.	*show ldp l2vpn fec*

3 Configuration Examples

This section provides L2VPN configuration examples in the following sections:

3.1 Static L2VPN

The following example configures a typical static L2VPN on a local PE router and a remote PE router. For this example, the L2VPN cross-connects 802.1Q PVCs.

The static L2VPN configuration for the local PE router is as follows:

```
[local]PE_Router(config)#context local

[local]PE_Router(config-ctx)#interface foo

[local]PE_Router(config-if)#ip address 200.2.2.2/32

[local]PE_Router(config-if)#exit

[local]PE_Router(config-ctx)#l2vpn

[local]PE_Router(config-l2vpn)#xc-group bar

[local]PE_Router(config-l2vpn-xc-group)#xc 4/1 vlan-id 300 vpn-label 5000
peer 100.1.1.1

[local]PE_Router(config-l2vpn-xc-group)#exit

[local]PE_Router(config-l2vpn)#exit

[local]PE_Router(config)#port ethernet 4/1

[local]PE_Router(config-port)#no shutdown

[local]PE_Router(config-port)#encapsulation dot1q

[local]PE_Router(config-port)#dot1q pvc 300

[local]PE_Router(config-dot1q-pvc)#l2vpn local
```

The static L2VPN configuration for the remote PE router is as follows:

```
[local]PE_Router(config)#context local

[local]PE_Router(config-ctx)#interface foo

[local]PE_Router(config-if)#ip address 100.1.1.1/31

[local]PE_Router(config-if)#exit

[local]PE_Router(config-ctx)#l2vpn

[local]PE_Router(config-l2vpn)#xc-group bar

[local]PE_Router(config-l2vpn-xc-group)#xc 4/1 vlan-id 300 vpn-label 5000
peer 100.1.1.1

[local]PE_Router(config-l2vpn-xc-group)#exit

[local]PE_Router(config-l2vpn)#exit

[local]PE_Router(config)#port ethernet 4/1

[local]PE_Router(config-port)#no shutdown

[local]PE_Router(config-port)#encapsulation dot1q

[local]PE_Router(config-port)#dot1q pvc 300

[local]PE_Router(config-dot1q-pvc)#l2vpn local
```

3.2 LDP L2VPN

The LDP L2VPN configuration examples assume that the following conditions are true:

- MPLS core backbone configuration is up and running.

  For more information on configuring MPLS, see *Configuring MPLS*.

- LDP targeted discovery has been enabled between PE peers.

  For more information on configuring LDP targeted discovery, see the *Targeted LDP* section in *Configuring LDP*.

The following LDP L2VPN examples configure LDP L2VPN on a local PE router and a remote PE router using the following encapsulation types:

- LDP L2VPN with Frame Relay Martini Encapsulation
- LDP L2VPN with Ethernet VLAN Encapsulation

- LDP L2VPN with Ethernet Encapsulation
- LDP L2VPN with ATM OC Encapsulation

3.2.1 LDP L2VPN with Frame Relay Martini Encapsulation

The following example demonstrates how two PE routers (**PE1** and **PE2**) are configured to correctly operate LDP L2VPN using Frame Relay Martini encapsulation.

Figure 4 displays the network topology for this example.

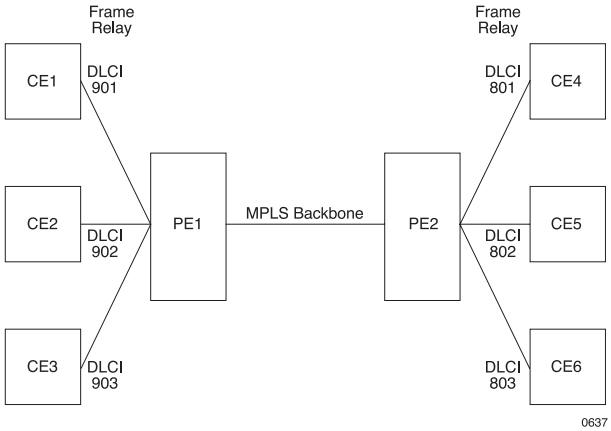

Figure 4 LDP L2VPN with Frame Relay Martini Encapsulation Network Topology

Note: Though the Frame Relay PVCs are different on the two sides, the VC IDs are still the same.

The configuration for the **PE1** router is as follows:

```
[local]PE1(config)#context local
[local]PE1(config-ctx)#no ip domain-lookup
[local]PE1(config-ctx)#interface loop1 loopback
[local]PE1(config-if)#ip address 11.200.1.2/32
[local]PE1(config-if)#exit
[local]PE1(config-ctx)#l2vpn
[local]PE1(config-l2vpn)#xc-group foo
[local]PE1(config-l2vpn-xc-group)#xc 12/4 dlci 901 vc-id 901 peer 11.200.1.1
[local]PE1(config-l2vpn-xc-group)#xc 12/4 dlci 902 vc-id 902 peer 11.200.1.1
[local]PE1(config-l2vpn-xc-group)#xc 12/4 dlci 903 vc-id 903 peer 11.200.1.1
[local]PE1(config-l2vpn-xc-group)#exit
[local]PE1(config-l2vpn)#exit
[local]PE1(config-ctx)#exit
[local]PE1(config)#port pos 12/4
[local]PE1(config-port)#no shutdown
[local]PE1(config-port)#encapsulation frame-relay
[local]PE1(config-port)#frame-relay pvc 901
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#frame-relay pvc 902
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#frame-relay pvc 903
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#end
```

The configuration for the **PE2** router is as follows:

```
[local]PE2(config)#context local
[local]PE2(config-ctx)#no ip domain-lookup
[local]PE2(config-ctx)#interface loop1 loopback
[local]PE2(config-if)#ip address 11.200.1.1/32
[local]PE2(config-if)#exit
[local]PE2(config-ctx)#router ldp
[local]PE2(config-ldp)#neighbor 11.200.1.2 targeted
[local]PE2(config-ldp)#exit
[local]PE2(config-ctx)#l2vpn
[local]PE2(config-l2vpn)#xc-group foo
[local]PE2(config-l2vpn-xc-group)#xc 12/3 dlci 801 vc-id 901 peer 11.200.1.2
[local]PE2(config-l2vpn-xc-group)#xc 12/3 dlci 802 vc-id 902 peer 11.200.1.2
[local]PE2(config-l2vpn-xc-group)#xc 12/3 dlci 803 vc-id 903 peer 11.200.1.2
[local]PE2(config-l2vpn-xc-group)#exit
[local]PE2(config-l2vpn)#exit
[local]PE2(config-ctx)#exit
[local]PE2(config)#port pos 12/3
[local]PE2(config-port)#no shutdown
[local]PE2(config-port)#encapsulation frame-relay
[local]PE2(config-port)#frame-relay pvc 801
[local]PE2(config-port)#l2vpn local
[local]PE2(config-port)#frame-relay pvc 802
[local]PE2(config-port)#l2vpn local
[local]PE2(config-port)#frame-relay pvc 803
[local]PE2(config-port)#l2vpn local
[local]PE2(config-port)#end
```

3.2.2 LDP L2VPN with Ethernet VLAN Encapsulation

The following example demonstrates how two PE routers (**PE1** and **PE2**) are configured to correctly operate LDP L2VPN using Ethernet VLAN encapsulation.

Note: The two CE ends use either the same or different dot1q PVCs in this example.

Figure 5 displays the network topology for this example.

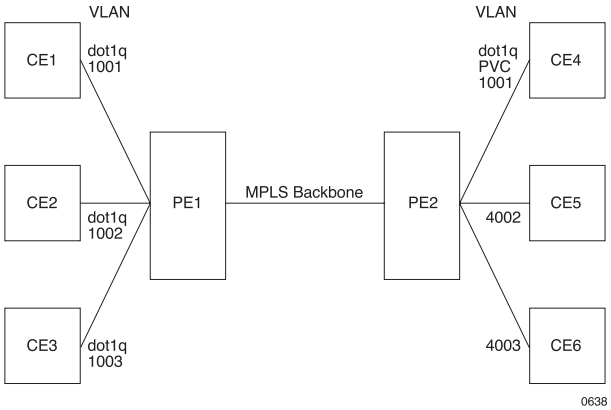

Figure 5 LDP L2VPN with Ethernet VLAN Encapsulation Network Topology

The configuration for the **PE1** router is as follows:

```
[local]PE1(config)#context local

[local]PE1(config-ctx)#interface loop1 loopback

[local]PE1(config-if)#ip address 11.200.1.2/32

[local]PE1(config-if)#exit

[local]PE1(config-ctx)#router ldp

[local]PE1(config-ldp)#neighbor 11.200.1.1 targeted

[local]PE1(config-ldp)#exit

[local]PE1(config-ctx)#l2vpn

[local]PE1(config-l2vpn)#xc-group foo

[local]PE1(config-l2vpn-xc-group)#xc 10/2 vlan-id 1001 vc-id 1001
peer 11.200.1.1
```

```
[local]PE1(config-l2vpn-xc-group)#xc 10/2 vlan-id 1002 vc-id 1002

[local]PE1(config-l2vpn-xc-group)#xc 10/2 vlan-id 1003 vc-id 1003
peer 11.200.1.1
[local]PE1(config-l2vpn-xc-group)#exit
[local]PE1(config-l2vpn)#exit
[local]PE1(config-ctx)#exit
[local]PE1(config)#card gigaether-4-port 10
[local]PE1(config)#port ethernet 10/2
[local]PE1(config-port)#no shutdown
[local]PE1(config-port)#encapsulation dot1q
[local]PE1(config-port)#dot1q pvc 1001
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#dot1q pvc 1002
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#dot1q pvc 1003
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#end
```

The configuration for the **PE2** router is as follows:

```
[local]PE2(config)#context local
[local]PE2(config-ctx)#no ip domain-lookup
[local]PE2(config-ctx)#interface loop1 loopback
[local]PE2(config-if)#ip address 11.200.1.1/32
[local]PE2(config-if)#exit
[local]PE2(config-ctx)#router ldp
[local]PE2(config-ldp)#neighbor 11.200.1.2 targeted
```

```
[local]PE2(config-ldp)#exit

[local]PE2(config-ctx)#l2vpn

[local]PE2(config-l2vpn)#xc-group foo

[local]PE2(config-l2vpn-xc-group)#xc 10/3 vlan-id 1001 vc-id 1001
peer 11.200.1.1

[local]PE2(config-l2vpn-xc-group)#xc 10/3 vlan-id 4002 vc-id 1002
peer 11.200.1.1

[local]PE2(config-l2vpn-xc-group)#xc 10/3 vlan-id 4003 vc-id 1003
peer 11.200.1.1

[local]PE2(config-l2vpn-xc-group)#exit

[local]PE2(config-l2vpn)#exit

[local]PE2(config-ctx)#exit

[local]PE2(config)#port ethernet 10/3

[local]PE2(config-port)#no shutdown

[local]PE2(config-port)#encapsulation dot1q

[local]PE2(config-port)#dot1q pvc 1001

[local]PE2(config-port)#l2vpn local

[local]PE2(config-port)#dot1q pvc 4002

[local]PE2(config-port)#l2vpn local

[local]PE2(config-port)#dot1q pvc 4003

[local]PE2(config-port)#l2vpn local

[local]PE2(config-port)#end
```

3.2.3 LDP L2VPN with Ethernet Encapsulation

The following example demonstrates how two PE routers (**PE1** and **PE2**) are configured to correctly operate LDP L2VPN using Ethernet encapsulation.

The configuration for the **PE1** router is as follows:

```
[local]PE1(config)#context local
[local]PE1(config-ctx)#no ip domain-lookup
[local]PE1(config-ctx)#interface loop1 loopback
[local]PE1(config-if)#ip address 11.200.1.1/32
[local]PE1(config-if)#exit
[local]PE1(config-ctx)#exit
[local]PE1(config)#l2vpn
[local]PE1(config-l2vpn)#xc-group foo
[local]PE1(config-l2vpn-xc-group)#xc 10/2 vc-id 1001 peer 11.200.1.2
[local]PE1(config-l2vpn-xc-group)#xc 10/4 vc-id 1002 peer 11.200.1.2
[local]PE1(config-l2vpn-xc-group)#exit
[local]PE1(config-l2vpn)#exit
[local]PE1(config-ctx)#exit
[local]PE1(config)#card gigaether-4-port 10
[local]PE1(config)#port ethernet 10/2
[local]PE1(config-port)#no shutdown
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#exit
[local]PE1(config)#port ethernet 10/4
[local]PE1(config-port)#no shutdown
[local]PE1(config-port)#l2vpn local
[local]PE1(config-port)#end
```

The configuration for the **PE2** router is as follows:

```
[local]PE2(config)#context local
[local]PE2(config-ctx)#no ip domain-lookup
[local]PE2(config-ctx)#interface loop1 loopback
[local]PE2(config-if)#ip address 11.200.1.2/32
[local]PE2(config-if)#exit
[local]PE2(config-ctx)#exit
[local]PE2(config)#l2vpn
[local]PE2(config-l2vpn)#xc-group foo
[local]PE2(config-l2vpn-xc-group)#xc 10/1 vc-id 1001 peer 11.200.1.1
[local]PE2(config-l2vpn-xc-group)#xc 10/3 vc-id 1002 peer 11.200.1.1
[local]PE2(config-l2vpn-xc-group)#exit
[local]PE2(config-l2vpn)#exit
[local]PE2(config-ctx)#exit
[local]PE2(config)#card gigaether-4-port 10
[local]PE2(config)#port ethernet 10/1
[local]PE2(config-port)#no shutdown
[local]PE2(config-port)#l2vpn local
[local]PE2(config-port)#exit
[local]PE2(config)#port ethernet 10/3
[local]PE2(config-port)#no shutdown
[local]PE2(config-port)#l2vpn local
[local]PE2(config-port)#end
```

3.2.4 LDP L2VPN with ATM OC Encapsulation

The following example demonstrates how two PE routers (**PE1** and **PE2**) are configured to correctly operate LDP L2VPN using ATM OC encapsulation.

The configuration for the **PE1** router is as follows:

```
[local]PE1(config)#context local

[local]PE1(config-ctx)#no ip domain-lookup

[local]PE1(config-ctx)#l2vpn

[local]PE1(config-l2vpn)#xc-group foo

[local]PE1(config-l2vpn-xc-group)#xc 5/1:1 vpi-vci 101 101 vc-id 101
peer 11.200.1.2

[local]PE1(config-l2vpn-xc-group)#exit

[local]PE1(config-l2vpn)#exit

[local]PE1(config-ctx)#exit

[local]PE1(config)#atm profile l2vpn-atm

[local]PE1(config-atmpro)#counters l2

[local]PE1(config-atmpro)#shaping ubr

[local]PE1(config-atmpro)#exit

[local]PE1(config)#port atm 5/1

[local]PE1(config-atm)#no shutdown

[local]PE1(config-atm)#atm pvc 101 101 profile l2vpn-atm encap bridge1483

[local]PE1(config-atmpvc)#l2vpn local

[local]PE1(config-atmpvc)#end
```

The configuration for the **PE2** router is as follows:

```
[local]PE2(config)#context local

[local]PE2(config-ctx)#l2vpn

[local]PE2(config-l2vpn)#xc-group foo

[local]PE2(config-l2vpn-xc-group)#xc 5/1:1 vpi-vci 101 101 vc-id 101
 peer 11.200.1.1

[local]PE2(config-l2vpn-xc-group)#exit

[local]PE2(config-l2vpn)#exit

[local]PE2(config-ctx)#exit

[local]PE2(config)#atm profile l2vpn-atm

[local]PE2(config-atmpro)#counters l2

[local]PE2(config-atmpro)#shaping ubr

[local]PE2(config)#port atm 5/1

[local]PE2(config-atm)#no shutdown

[local]PE2(config-atm)#atm pvc 101 101 profile l2vpn-atm encap bridge1483

[local]PE2(config-atmpvc)#l2vpn local

[local]PE2(config-atmpvc)#end
```

3.3 CE Router with RFC 1483 Bridged Encapsulation for ATM AAL5

The following example configures a CE router with RFC 1483 bridged encapsulation for ATM AAL5:

```
[local]CE(config)#context CE1-atm-ds3-104

[local]CE(config-ctx)#no ip domain-lookup

[local]CE(config-ctx)#interface ce1-atm-ds3-104

[local]CE(config-if)#ip address 104.1.1.1/24

[local]CE(config-if)#exit

[local]CE(config-ctx)#exit

[local]CE(config)#atm profile l2vpn-atm-ds3

[local]CE(config-atmpro)#counters l2

[local]CE(config-atmpro)#shaping ubr

[local]CE(config-atmpro)#exit

[local]CE(config)#port atm 4/7

[local]CE(config-atm)#no shutdown

[local]CE(config-atm)#atm pvc 104 104 profile l2vpn-atm-ds3 encap bridge1483

[local]CE(config-atmpvc)#bind interface ce1-atm-ds3-104 CE1-atm-ds3-104

[local]CE(config-atmpvc)#end
```

3.4 L2VPN for Extreme Networks Equipment Interoperability

This setup is used for testing interoperability with Extreme Networks switches' VMAN-type packets. The L2VPN does not require a specific configuration for this example. Extreme Networks switches use 9100 as the Ethertype for these configurations.

For this example, SmartEdge routers are used as PE routers. The **CE1** router is connected to the **PE1** router through an Extreme Networks **Summit5si** switch. The ingress port for the tunnel is **1** and egress port on the VMAN tunnel on the **Summit5i** is **2**. The **PE2** router is connected to the **CE2** router through an Extreme Networks **Summit24** switch. The **PE2** router's port is Gigabit Ethernet, but the **CE2** router's port is Ethernet; they are connected together over a VLAN/VMAN configuration.

Figure 6 displays the network topology for this configuration example.

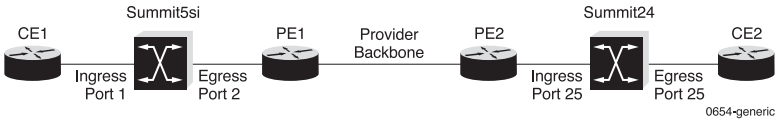

Figure 6 Network Topology for Extreme Networks Equipment Interoperability

This setup uses the same VLAN ID on both ends, but should also work properly with different VLAN IDs.

Note: This example does not show the MPLS Layer 3 backbone configuration. See *Configuring MPLS* for MPLS backbone configuration examples.

The L2VPN configuration for the Extreme Networks **Summit5si** switch is as follows:

```
configure dot1q ethertype 9100
create vlan "l2vpn-CE1"
# Config information for VLAN l2vpn-CE1.
config vlan "l2vpn-CE1" tag 1000     # VLAN-ID=0x3e8 Global Tag 72
config vlan "l2vpn-CE1" protocol "ANY"
config vlan "l2vpn-CE1" qosprofile "QP1"
# No IP address is configured for VLAN l2vpn-CE1.
configure vlan "l2vpn-CE1" add port 1 untagged
config vlan "l2vpn-CE1" add port 2 tagged
configure jumbo-frame size 1530
disable red port 1
disable dlcs port 1
configure port 1 auto on
enable jumbo-frame ports 1
enable edp port 1
disable red port 2
disable dlcs port 2
configure port 2 auto on
enable jumbo-frame ports 2
```

The L2VPN configuration for the **CE1** router is as follows:

```
[local]CE1#config
[local]CE1(config)#context CE1-extreme-1000
[local]CE1(config-ctx)#no ip domain-lookup
[local]CE1(config-ctx)#interface ce1-extreme-1000
[local]CE1(config-if)#ip address 1.1.1.1/24
[local]CE1(config-if)#exit
[local]CE1(config-ctx)#exit
[local]CE1(config)#port ethernet 10/2
[local]CE1(config-port)#no shutdown
[local]CE1(config-port)#encapsulation dot1q
[local]CE1(config-port)#dot1q pvc 1000
[local]CE1(config-port)#bind interface ce1-extreme-1000 CE1-extreme-1000
[local]CE1(config-port)#end
```

The L2VPN configuration for the **PE1** router is as follows:

```
[local]PE1#config

[local]PE1(config)#context local

[local]PE1(config-ctx)#interface loop1 loopback

[local]PE1(config-if)#ip address 11.200.1.2/32

[local]PE1(config-if)#exit

[local]PE1(config-ctx)#router ldp

[local]PE1(config-ldp)#neighbor 11.200.1.1 targeted

[local]PE1(config-ldp)#exit

[local]PE1(config-ctx)#l2vpn

[local]PE1(config-l2vpn)#xc-group foo

[local]PE1(config-l2vpn-xc-group)#xc 10/1 vlan-id 1000 vc-id 1000
peer 11.200.1.1

[local]PE1(config-l2vpn-xc-group)#exit

[local]PE1(config-l2vpn)#exit

[local]PE1(config-ctx)#exit

[local]PE1(config)#card gigaether-4-port 10

[local]PE1(config)#port ethernet 10/1

[local]PE1(config-port)#description to-Extereme-port2

[local]PE1(config-port)#no shutdown

[local]PE1(config-port)#encapsulation dot1q

[local]PE1(config-port)#dot1q pvc 1000

[local]PE1(config-port)#l2vpn local

[local]PE1(config-port)#end
```

The L2VPN configuration for the **PE2** router is as follows:

```
[local]PE2(config)#context local

[local]PE2(config-ctx)#interface loop1 loopback

[local]PE2(config-if)#ip address 11.200.1.1/32

[local]PE2(config-if)#exit

[local]PE2(config-ctx)#router ldp

[local]PE2(config-ldp)#neighbor 11.200.1.2 targeted

[local]PE2(config-ldp)#exit

[local]PE2(config-ctx)#l2vpn

[local]PE2(config-l2vpn)#xc-group foo

[local]PE2(config-l2vpn-xc-group)#xc 10/2 vlan-id 1000 vc-id 1000
peer 11.200.1.2

[local]PE2(config-l2vpn-xc-group)#exit

[local]PE2(config-l2vpn)#exit

[local]PE2(config-ctx)#exit

[local]PE2(config)#port ethernet 10/2

[local]PE2(config-port)#no shutdown

[local]PE2(config)#encapsulation dot1q

[local]PE2(config-port)#dot1q pvc 1000

[local]PE2(config-port)#l2vpn local

[local]PE2(config-port)#end
```

The L2VPN configuration for the **CE2** router is as follows:

```
[local]CE2(config)#context CE2-FE-dot1q-1000
[local]CE2(config-ctx)#no ip domain-lookup
[local]CE2(config-ctx)#interface ce2-fe-dot1q-1000
[local]CE2(config-if)#ip address 1.1.1.2/24
[local]CE2(config-if)#exit
[local]CE2(config-ctx)#exit
[local]CE2(config)#card ge-10-port 14
[local]CE2(config)#port ethernet 14/1
[local]CE2(config-port)#no shutdown
[local]CE2(config-port)#encapsulation dot1q
[local]CE2(config-port)#dot1q pvc 1000
[local]CE2(config-port)#bind interface ce2-fe-dot1q-1000 CE2-FE-dot1q-1000
[local]CE2(config-port)#end
```

The L2VPN configuration on the Extreme Networks Summit 24 switch is as follows:

```
configure dot1q ethertype 9100
enable jumbo
# Config information for VLAN l2vpn-CE2.
config vlan "l2vpn-CE2" tag 1000     # VLAN-ID=0x3e8 Global Tag 256
config vlan "l2vpn-CE2" protocol "ANY"
config vlan "l2vpn-CE2" qosprofile "QP1"
# No IP address is configured for VLAN l2vpn-CE2.
configure vlan "l2vpn-CE2" add port 2 untagged
config vlan "l2vpn-CE2" add port 25 tagged
```

3.5 ATM-to-ATM Pseudowire Cross-Connection

The SmartEdge router supports L2VPN pseudowire cross-connectivity between two ATM circuits. The pseudowire can carry a single PVC or multiple PVCs.

This section provides examples of configuring an ATM pseudowire cross-connection with a single or multiple PVCs.

3.5.1 ATM Pseudowire Cross-Connection with a Single PVC

The following example shows how to configure an ATM pseudowire cross-connection that carries a single PVC.

Configure the ATM circuit between the CE router and the first PE router (PE1):

```
[local]PE1#configure
Enter configuration commands, one per line, 'end' to exit
[local]PE1(config)#port atm 4/1
[local]PE1(config-atm-oc)#atm pvc 0 32 profile atm-prof1 encapsulation cell
[local]PE1(config-atm-pvc)#l2vpn local
[local]PE1(config-atm-pvc)#end
```

Configure one end of the pseudowire cross-connection on the first PE router (PE1):

```
[local]PE1(config)#configure
[local]PE1(config)#context local
[local]PE1(config-ctx)#l2vpn
[local]PE1(config-l2vpn)#xc-group group2
[local]PE1(config-l2vpn-xc-group)#control-word sequence-number
[local]PE1(config-l2vpn-xc-group)#xc 4/2 vpi-vci 0 32 vc-id 20000
peer 111.111.111.111 cell-encap nto1-vcc
```

Configure the ATM circuit on the second PE router (PE2):

```
[local]PE2#configure

Enter configuration commands, one per line, 'end' to exit

[local]PE2(config)#port atm 2/2

[local]PE2(config-atm-oc)#atm pvc 0 32 profile atm-prof1 encapsulation cell

[local]PE2(config-atm-pvc)#l2vpn local

[local]PE2(config-atm-pvc)#end
```

Configure the pseudowire cross-connection between the ATM circuits on the PE routers. Perform this configuration on the second router:

```
[local]PE2(config)#configure

[local]PE2(config)#context local

[local]PE2(config-ctx)#l2vpn

[local]PE2(config-l2vpn)#xc-group group2

[local]PE2(config-l2vpn-xc-group)#control-word sequence-number

[local]PE2(config-l2vpn-xc-group)#xc 4/2 vpi-vci 0 32 vc-id 20000
peer 111.111.111.111 cell-encap nto1-vcc
```

3.5.2 ATM Pseudowire Cross-Connection with Multiple PVCs

The following example shows how to configure an ATM pseudowire cross-connection that carries multiple PVCs.

Configure the ATM circuit between the CE router and the first PE router (PE1):

```
[local]PE1(config)#port atm 4/1

[local]PE1(config-atm-oc)#atm pvc explicit 0:32 through 0:8000 profile
atm-prof1 encapsulation cell

[local]PE1(config-atm-pvc)#l2vpn local

[local]PE2(config-atm-pvc)# end
```

Configure one end of the pseudowire cross-connection on the first PE router (PE1):

```
[local]PE1(config)#configure

[local]PE1(config)#context local

[local]PE1(config-ctx)#l2vpn

[local]PE1(config-l2vpn)#xc-group group1

[local]PE1(config-l2vpn-xc-group)#xc 4/1 vpi-vci 0 32 through 8000 n-to-1
 vc-id 1 peer 1.1.1.1 cell-encap nto1-vcc

[local]PE2(config-l2vpn-xc-group)#end
```

Configure the ATM circuit on the second PE router (PE2):

```
[local]PE2(config)#port atm 4/1

[local]PE2(config-atm-oc)#atm pvc explicit 0:32 through 0:8000
profile atm-prof1 encapsulation cell

[local]PE2(config-atm-pvc)#l2vpn local

[local]PE2(config-atm-pvc)#end
```

Configure the pseudowire cross-connection between the ATM circuits on the PE routers. Perform this configuration on the second PE router (PE2):

```
[local]PE2(config)#configure

[local]PE2(config)#context local

[local]PE2(config-ctx)#l2vpn

[local]PE2(config-l2vpn)#xc-group group1

[local]PE2(config-l2vpn-xc-group)#xc 4/1 vpi-vci 0 32 through 8000
n-to-1 vc-id 1 peer 1.1.1.1 cell-encap nto1-vcc

[local]PE2(config-l2vpn-xc-group)#end
```

3.6 1483 Routed ATM-to-Ethernet Interconnection

The SmartEdge router supports L2VPN cross-connectivity when one end of the cross-connection is an ATM RFC 1483 routed circuit and the other end is an Ethernet circuit. The Ethernet circuit can be pure Ethernet or dot1q.

This section provides examples of configuring pseudowire cross-connections between a 1483 routed ATM circuit and a pure Ethernet circuit or between a 1483 routed ATM circuit and a dot1q VLAN circuit.

3.6.1 Pseudowire Cross-Connection Between a 1483 Routed ATM Circuit and a Pure Ethernet Circuit

The following example shows how to configure an interconnection between an ATM RFC 1483 routed circuit and a pure Ethernet circuit on two sides of an L2VPN pseudowire cross-connection.

Configure the ATM circuit between the CE router and the first PE router (`PE1`):

```
[local]PE1(config)#port atm 4/2

[local]PE1(config-atm-oc)#atm pvc 0 32 profile atm-prof1
encapsulation route1483

[local]PE1(config-atm-pvc)#l2vpn local

[local]PE1(config-atm-pvc)#end
```

Configure one end of the pseudowire cross-connection on the first PE router. This PE router connects to the ATM CE router:

```
[local]PE1(config)#context local

[local]PE1(config-ctx)#l2vpn

[local]PE1(config-l2vpn)#xc-group 1483

[local]PE1(config-l2vpn-xc-group)#xc 4/2 vpi-vci 0 32 vc-id 1
 peer 1.1.1.2 remote-encap ethernet

[local]PE1(config-l2vpn-xc-group)#end
```

Configure the Ethernet circuit on the second PE router (`PE2`):

```
[local]PE2(config)#port ethernet 10/1

[local]PE2(config-port)#l2vpn local

[local]PE2(config-port)#end
```

Configure the pseudowire cross-connection between the Ethernet circuit and the ATM circuit. Perform this configuration on the second router (the router that connects to the Ethernet CE router). After you commit this configuration, the pseudowire is active:

```
[local]PE2(config)#context local

[local]PE2(config-ctx)#l2vpn

[local]PE2(config-l2vpn)#xc-group foo

[local]PE2(config-l2vpn-xc-group)#xc 10/1 vc-id 1 peer 1.1.1.1

[local]PE2(config-l2vpn-xc-group)#end
```

3.6.2 Pseudowire Cross-Connection Between a 1483 Routed ATM Circuit and a dot1q VLAN Circuit

The following example shows how to configure an interconnection between an ATM RFC 1483 routed circuit and a dot1q VLAN circuit on two sides of an L2VPN pseudowire cross-connection.

Configure the ATM circuit between the CE router and the first PE router (`PE1`):

```
[local]PE1(config)#port atm 4/2

[local]PE1(config-atm-oc)#atm pvc 0 32 profile atm-prof1
encapsulation route1483

[local]PE1(config-atm-pvc)#l2vpn local

[local]PE1(config-atm-pvc)#end
```

Configure one end of the pseudowire cross-connection on the first PE router. This PE router connects to the ATM CE router:

```
[local]PE1(config)#context local

[local]PE1(config-ctx)#l2vpn

[local]PE1(config-l2vpn)#xc-group 1483

[local]PE1(config-l2vpn-xc-group)#xc 4/2 vpi-vci 0 32 vc-id 1 peer 1.1.1.2
 remote-encap ethernet

[local]PE1(config-l2vpn-xc-group)#end
```

Configure the VLAN circuit on the second PE router (PE2):

```
[local]PE2(config)#port ethernet 10/1

[local]PE2(config-port)#encapsulation dot1q

[local]PE2(config-port)#dot1q pvc 1

[local]PE2(config-dot1q-pvc)#l2vpn local

[local]PE2(config-dot1q-pvc)#end
```

Configure the pseudowire cross-connection between the VLAN circuit and the ATM circuit. Perform this configuration on the second router (the router that connects to the Ethernet CE router). After you commit this configuration, the pseudowire is active:

```
[local]PE2(config)#context local

[local]PE2(config-ctx)#l2vpn

[local]PE2(config-l2vpn)#xc-group foo

[local]PE2(config-l2vpn-xc-group)#xc 10/1 vlan-id 1 vc-id 1 peer 1.1.1.1
remote-encap ethernet

[local]PE2(config-l2vpn-xc-group)#end
```

3.7 Ethernet Resiliency

The following example shows how to configure Ethernet resiliency on a pseudowire between two PE routers.

Configure the port on the first PE router. In this example, the user brings up an individual dot1q port:

```
[local]PE_Router(config)#port ethernet 1/1

[local]PE_Router(config-port)#no shutdown

[local]PE_Router(config-port)#encapsulation dot1q

[local]PE_Router(config-port)#dot1q pvc 300

[local]PE_Router(config-dot1q-pvc)#l2vpn local
```

Configure a cross-connection group on the first PE router:

```
[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group group_1

[local]Redback(config-l2vpn-xc-group)# xc 1/1 vlan-id 300 vc-id 1002
peer 2.2.2.2

[local]Redback(config-l2vpn-xc-group)# xc link_group_1 vlan-id 10 vc-id 1001
peer 2.2.2.2

[local]Redback(config-l2vpn-xc-group)# xc link_group_2 vlan-id 20 vc-id 1001
peer 2.2.2.2
```

Configure the port on the second PE router. In this example, the user brings up an individual dot1q port:

```
[local]PE_Router(config)#port ethernet 4/1

[local]PE_Router(config-port)#no shutdown

[local]PE_Router(config-port)#encapsulation dot1q

[local]PE_Router(config-port)#dot1q pvc 95

[local]PE_Router(config-dot1q-pvc)#l2vpn local
```

Configure a cross-connection group on the second PE router. When you commit this configuration, the connection becomes active:

```
[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group group_2

[local]Redback(config-l2vpn-xc-group)# xc 4/1 vlan-id 200 vc-id 1002
peer 2.2.2.2

[local]Redback(config-l2vpn-xc-group)# xc link_group_1 vlan-id 30 vc-id 1001
peer 2.2.2.2

[local]Redback(config-l2vpn-xc-group)# xc link_group_2 vlan-id 40 vc-id 1001
peer 2.2.2.2
```

3.8 QoS Rate-Limiting Policy on Ingress L2VPN Circuits

The following example configures the QoS rate-limiting policy L2VPN for an ingress L2VPN circuit with Ethernet VLAN encapsulation. Incoming packets that exceed the 40000 kbps rate are dropped by default:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group foo

[local]Redback(config-l2vpn-xc-group)#xc 10/2 vlan-id 1001 vc-id 1001
peer 11.200.1.2

[local]Redback(config-l2vpn-xc-group)#exit

[local]Redback(config-l2vpn)#exit

[local]Redback(config-ctx)#exit

[local]Redback(config)#qos policy l2vpn policing

[local]Redback(config-qos-pol-rl)#rate 40000 burst 20000

[local]Redback(config-qos-pol-rate)#exit

[local]Redback(config-qos-pol-rl)#exit

[local]Redback(config)#port ethernet 10/2

[local]Redback(config-port)#no shutdown

[local]Redback(config-port)#encapsulation dot1q

[local]Redback(config-port)#dot1q pvc 1001

[local]Redback(config-dot1q-pvc)#l2vpn local

[local]Redback(config-dot1q-pvc)#qos policy l2vpn in
```

3.9 QoS Metering Policies on Egress L2VPN Circuits

The following example configures the QoS metering policy, **l2vpn-shaping**, on the egress side of an L2VPN cross-connection. Outgoing packets that exceed the **10000** rate are dropped:

```
[local]Redback#config
[local]Redback(config)#port ethernet 9/2
[local]Redback(config-port)#dot1q pvc 1
[local]Redback(config-pvc)#qos policy metering l2vpn-shaping
[local]Redback(config-pvc)#exit
[local]Redback(config-port)#exit
[local]Redback(config)#qos policy l2vpn-shaping metering
[local]Redback(config-qos-pol-rl)#rate 10000 burst 2000
[local]Redback(config-qos-pol-rl)#end
```

3.10 EXP-Bit for L2VPN VCs

EXP bits can be set for L2VPN virtual circuits (VCs) to be applied to the outgoing backbone queues. The EXP bit is set for the Layer 2 label and is then copied to the appropriate Layer 3 label. This sets the corresponding outgoing backbone queue. For information on QoS queues, see *Configuring Circuits for QoS* .

The following configuration example sets the EXP bits for L2VPN circuits.

Note: This example is a relevant partial configuration; for a complete Layer 3 configuration, see *Configuring MPLS*.

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#no ip domain-lookup
[local]Redback(config-ctx)#interface loop1 loopback
[local]Redback(config-if)#ip address 11.200.1.1/32
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#interface to-P
[local]Redback(config-if)#ip address 101.1.1.4/24
[local]Redback(config-if)#exit
```

```
[local]Redback(config-ctx)#router mpls
[local]Redback(config-mpls)#interface loop1
[local]Redback(config-mpls-if)#exit
[local]Redback(config-mpls)#interface to-P
[local]Redback(config-mpls-if)#exit
[local]Redback(config-mpls)#exit
[local]Redback(config-ctx)#router rsvp
[local]Redback(config-rsvp-explicit-route)#explicit-route to-MPLS2-via-P
[local]Redback(config-rsvp-explicit-route)#next-hop 101.1.1.5
[local]Redback(config-rsvp-explicit-route)#next-hop 4.1.1.5
[local]Redback(config-rsvp-explicit-route)#exit
[local]Redback(config-rsvp)#lsp S4_P_S2
[local]Redback(config-rsvp-lsp)#ingress 11.200.1.1
[local]Redback(config-rsvp-lsp)#egress 11.200.1.2
[local]Redback(config-rsvp-lsp)#source-path to-MPLS2-via-P
[local]Redback(config-rsvp-lsp)#exit
[local]Redback(config-rsvp)#interface loop1
[local]Redback(config-rsvp-if)#exit
[local]Redback(config-rsvp)#interface to-P
[local]Redback(config-rsvp-if)#exit
[local]Redback(config-rsvp)#exit
[local]Redback(config-ctx)#router ldp
[local]Redback(config-ldp)#neighbor 11.200.1.2 targeted
[local]Redback(config-ldp)#exit
[local]Redback(config-ctx)#l2vpn
[local]Redback(config-l2vpn)#xc-group foo
```

```
[local]Redback(config-l2vpn-xc-group)#xc 10/2 vlan-id 4001 vc-id 4001
peer 11.200.1.2 exp-bits 7

[local]Redback(config-l2vpn-xc-group)#xc 10/2 vlan-id 4002 vc-id 4002
peer 11.200.1.2 exp-bits 6

[local]Redback(config-l2vpn-xc-group)#xc 10/2 vlan-id 4003 vc-id 4003
peer 11.200.1.2 exp-bits 5

[local]Redback(config-l2vpn-xc-group)#exit

[local]Redback(config-l2vpn)#exit

[local]Redback(config-ctx)#exit

[local]Redback(config)#qos queue-map default

[local]Redback(config-queue-map)#num-queues 2

[local]Redback(config-qos-queue-map-num-queues)#queue 0 priority 0

[local]Redback(config-qos-queue-map-num-queues)#queue 1 priority 1 2 3 4 5 6 7

[local]Redback(config-qos-queue-map-num-queues)#exit

[local]Redback(config-queue-map)#num-queues 4

[local]Redback(config-qos-queue-map-num-queues)#queue 0 priority 0

[local]Redback(config-qos-queue-map-num-queues)#queue 1 priority 1 2

[local]Redback(config-qos-queue-map-num-queues)#queue 2 priority 3 4 5 6

[local]Redback(config-qos-queue-map-num-queues)#queue 3 priority 7

[local]Redback(config-qos-queue-map-num-queues)#exit

[local]Redback(config-queue-map)#num-queues 8

[local]Redback(config-qos-queue-map-num-queues)#queue 0 priority 0

[local]Redback(config-qos-queue-map-num-queues)#queue 1 priority 1

[local]Redback(config-qos-queue-map-num-queues)#queue 2 priority 2

[local]Redback(config-qos-queue-map-num-queues)#queue 3 priority 3

[local]Redback(config-qos-queue-map-num-queues)#queue 4 priority 4

[local]Redback(config-qos-queue-map-num-queues)#queue 5 priority 5
```

```
[local]Redback(config-qos-queue-map-num-queues)#queue 6 priority 6
[local]Redback(config-qos-queue-map-num-queues)#queue 7 priority 7
[local]Redback(config-qos-queue-map-num-queues)#exit
[local]Redback(config-queue-map)#exit
[local]Redback(config)#qos policy pq2 pwfq
[local]Redback(config)#port ethernet 10/2
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#encapsulation dot1q
[local]Redback(config-port)#dot1q pvc 4001
[local]Redback(config-dot1q-pvc)#l2vpn local
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 4002
[local]Redback(config-dot1q-pvc)#l2vpn local
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#dot1q pvc 4003
[local]Redback(config-dot1q-pvc)#l2vpn local
[local]Redback(config-dot1q-pvc)#exit
[local]Redback(config-port)#exit
[local]Redback(config)#port ethernet 10/3
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#bind interface to-P local
[local]Redback(config-port)#qos policy queuing pq2
```

3.11 Example of dot1q Bit Propagation on L2VPN Cross-Connections

L2VPN circuits support propagating dot1p bits to EXP bits on ingress routers, and EXP bits to dot1p bits on egress router. When a dot1q profile is applied to an ingress L2VPN circuit, the dot1p bits are propagated to QoS bits, and then MPLS propagates the QoS bits to the EXP bits, for both L2 and L3 labels. When the dot1p profile is applied to an egress L2VPN circuit, MPLS propagates the EXP bits to the QoS bits, and then the QoS bits are propagated to the dot1p bits.

The following example propagates dot1p bits to EXP bits by applying the **dot1q-qos** dot1q profile to an ingress L2VPN circuit:

```
[local]Redback#configure
[local]Redback(config)#dot1q profile dot1q-qos
[local]Redback(config-dot1q-profile)#propagate qos from ethernet
[local]Redback(config-dot1q-profile)#commit
[local]Redback(config-dot1q-profile)#exit
[local]Redback(config)#context local
[local]Redback(config-ctx)#router mpls
[local]Redback(config-mpls)#propagate qos to-mpls
[local]Redback(config-mpls)#commit
[local]Redback(config-mpls)#exit
[local]Redback(config)#port ethernet 9/2
[local]Redback(config-port)#dot1q pvc 1001 profile dpt1q-qos
[local]Redback(config-dot1q-pvc)#l2vpn local
[local]Redback(config-dot1q-pvc)#end
```

The following example propagates EXP bits to dot1p bits by applying the **qos-dot1q** dot1q profile to an egress L2VPN circuit:

```
[local]Redback#configure
[local]Redback(config#dot1q profile qos-dot1q
[local]Redback(config-dot1q-profile)#propagate qos to ethernet
[local]Redback(config-dot1q-profile)#commit
[local]Redback(config-dot1q-profile)#exit
[local]Redback(config)#context local
[local]Redback(config-ctx)#router mpls
[local]Redback(config-mpls)#propagate qos from-mpls
[local]Redback(config-mpls)#commit
[local]Redback(config-mpls)#exit
[local]Redback(config)#port ethernet 9/2
[local]Redback(config-port)#dot1q pvc 1001 profile qos-dot1q
[local]Redback(config-dot1q-pvc)#l2vpn local
[local]Redback(config-dot1q-pvc)#end
```

3.12 ATM RFC 1483 Bridged to dot1q Interconnection

The SmartEdge router supports L2VPN cross-connectivity when one end of the cross-connection is an ATM RFC 1483 bridged circuit, and the other end is a dot1q circuit. The following example configures an interconnection between ATM RFC 1483 bridged and dot1q on two sides of an L2VPN cross-connection. Figure 7 displays the network topology for this configuration example.

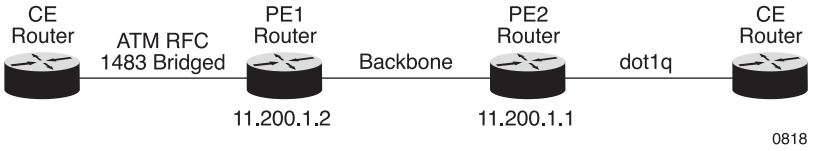

Figure 7 ATM RFC 1483 Bridged to dot1q Network Topology

The L2VPN configuration for the **PE1** router is as follows:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group foo

[local]Redback(config-l2vpn-xc-group)#xc 10/1:1 vpi-vci 104 104 vc-id 104
peer 11.200.1.1 remote-encap dot1q

[local]Redback(config-l2vpn-xc-group)#xc 10/1:1 vpi-vci 105 105 vc-id 105
peer 11.200.1.1 remote-encap dot1q

[local]Redback(config-l2vpn-xc-group)#xc 10/1:1 vpi-vci 106 106 vc-id 106
peer 11.200.1.1 remote-encap dot1q

[local]Redback(config-l2vpn-xc-group)#exit

[local]Redback(config-l2vpn)#exit

[local]Redback(config-ctx)#exit

[local]Redback(config)#port atm 10/1

[local]Redback(config-atm)#no shutdown

[local]Redback(config-atm)#atm pvc 104 104 profile l2vpn-atm encap bridge1483

[local]Redback(config-atmpvc)#l2vpn local

[local]Redback(config-atmpvc)#exit

[local]Redback(config-atm)#atm pvc 105 105 profile l2vpn-atm encap bridge1483

[local]Redback(config-atmpvc)#l2vpn local

[local]Redback(config-atmpvc)#exit

[local]Redback(config-atm)#atm pvc 106 106 profile l2vpn-atm encap bridge1483

[local]Redback(config-atmpvc)#l2vpn local

[local]Redback(config-atmpvc)#end
```

The L2VPN configuration for the **PE2** router is as follows:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group foo

[local]Redback(config-l2vpn-xc-group)#xc 5/1 vlan-id 1001 vc-id 104
peer 11.200.1.2 remote-encap bridge1483

[local]Redback(config-l2vpn-xc-group)#xc 5/1 vlan-id 1002 vc-id 105
peer 11.200.1.2 remote-encap bridge1483

[local]Redback(config-l2vpn-xc-group)#xc 5/1 vlan-id 1003 vc-id 106
peer 11.200.1.2 remote-encap bridge1483

[local]Redback(config-l2vpn-xc-group)#exit

[local]Redback(config-l2vpn)#exit

[local]Redback(config-ctx)#exit

[local]Redback(config)#port eth 5/1

[local]Redback(config-port)#no shutdown

[local]Redback(config-port)#encapsulation dot1q

[local]Redback(config-port)#dot1q pvc 1001

[local]Redback(config-dot1q-pvc)#l2vpn local

[local]Redback(config-dot1q-pvc)#exit

[local]Redback(config-port)#dot1q pvc 1002

[local]Redback(config-dot1q-pvc)#l2vpn local

[local]Redback(config-dot1q-pvc)#exit

[local]Redback(config-port)#dot1q pvc 1003

[local]Redback(config-dot1q-pvc)#l2vpn local

[local]Redback(config-dot1q-pvc)#end
```

3.13 ATM RFC 1483 Bridged to Ethernet Interconnection

The SmartEdge router supports L2VPN cross-connectivity when one end of the cross-connection is an ATM RFC 1483 bridged circuit, and the other end is an Ethernet circuit. The following example configures an interconnection between ATM RFC 1483 bridged and Ethernet on two sides of an L2VPN cross-connection.

Figure 8 displays the network topology for this configuration example.

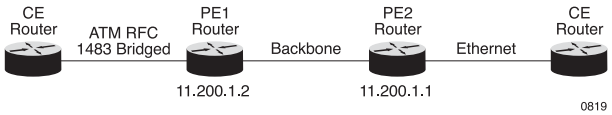

Figure 8 ATM RFC 1483 Bridged to Ethernet Network Topology

The L2VPN configuration for the **PE1** router is as follows:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group foo

[local]Redback(config-l2vpn-xc-group)#xc 13/1:1 vpi-vci 104 104 vc-id 1001
peer 11.200.1.1 remote-encap ethernet

[local]Redback(config-l2vpn-xc-group)#exit

[local]Redback(config-l2vpn)#exit

[local]Redback(config-ctx)#exit

[local]Redback(config)#port atm 13/1

[local]Redback(config-atm)#no shutdown

[local]Redback(config-atm)#atm pvc 104 104 profile l2vpn-atm
encapsulation bridge1483

[local]Redback(config-atmpvc)#l2vpn local

[local]Redback(config-atmpvc)#end
```

The L2VPN configuration for the **PE2** router is as follows:

```
[local]Redback#config

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group foo

[local]Redback(config-l2vpn-xc-group)#xc 10/3 vc-id 1001 peer 11.200.1.2
remote-encap bridge1483

[local]Redback(config-l2vpn-xc-group)#exit

[local]Redback(config-l2vpn)#exit

[local]Redback(config-ctx)#exit

[local]Redback(config)#port ethernet 10/3

[local]Redback(config-port)#no shutdown

[local]Redback(config-port)#l2vpn local

[local]Redback(config-port)#end
```

3.14 L2VPN over GRE

The SmartEdge router supports L2VPN over GRE, which is a method of transporting L2VPN-encapsulated packets using soft GRE tunnels. For L2VPN over GRE to work properly, the ingress and egress PE routers must both be configured to support soft GRE functionality. The following example enables soft GRE tunneling.

Figure 9 displays the network topology for this configuration example.

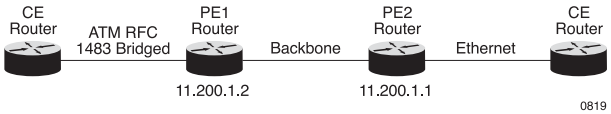

Figure 9 L2VPN over GRE Network Topology

The L2VPN over GRE configuration for the **PE1** router is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to_SJ_1
[local]Redback(config-if)#ip address 192.168.10.5/30
[local]Redback(config-if)# exit
[local]Redback(config-ctx)#router mpls
[local]Redback(config-mpls)#exit
[local]Redback(config-ctx)#ip soft-gre source 11.200.1.2
[local]Redback(config-ctx)#end
```

The L2VPN over GRE configuration for the **PE2** router is as follows:

```
[local]Redback#config
[local]Redback(config)#context local
[local]Redback(config-ctx)#interface to_SJ_2
[local]Redback(config-if)#ip address 192.165.10.5/20
[local]Redback(config-if)# exit
[local]Redback(config-ctx)#router mpls
[local]Redback(config-mpls)#exit
[local]Redback(config-ctx)#ip soft-gre source 11.200.1.1
[local]Redback(config-ctx)#end
```

3.15 L2VPN XC-to-MPLS LSP Mapping

This section provides examples of mapping an L2VPN XC to an LDP LSP, mapping an L2VPN XC to an RSVP LSP, and configuring an LSP to be exclusive.

3.15.1 Mapping an L2VPN XC to an LDP LSP

This section provides an example of how to map an L2VPN XC to an LDP LSP. First, create an L2VPN profile. In this example, the user creates an L2VPN profile called **it-test**. In the it-test profile, an LDP path is designated for L2VPN XC mapping:

```
[local]Redback#config

[local]Redback(config)#l2vpn profile it-test

[local]Redback(config-l2vpn-xc-profile)#peer 77.77.77.1

[local]Redback(config-l2vpn-xc-profile-peer)#tunnel ldp-path

[local]Redback(config-l2vpn-xc-profile-peer)#exit

[local]Redback(config-l2vpn-xc-profile)#exit
```

Next, reference the L2VPN profile in the configuration of the XC you want to map to the LSP that is designated in the profile. In the following example, the user references the “it-test” L2VPN profile in the in the configuration for XC 10/12:

```
[local]Redback(config-l2vpn-xc-group)#xc-group it-test

[local]Redback(config-l2vpn-xc-group)#xc 10/12 vc-id 111 profile it-test
```

3.15.2 Mapping an L2VPN XC to an RSVP LSP

This section provides an example of how to map an L2VPN XC to an RSVP LSP.

First, create an L2VPN profile. In this example, the user creates a profile called **troll1**, which designates the primary LSP tunnel for mapping, and specifies that encapsulation on the other end of the LSP must be Ethernet:

```
[local]Redback#config

[local]Redback(config)#l2vpn profile troll1

[local]Redback(config-l2vpn-xc-profile)##peer 20.20.20.20

[local]Redback(config-l2vpn-xc-profile-peer)#tunnel lsp primary

[local]Redback(config-l2vpn-xc-profile-peer)#remote-encap ethernet
```

Next, map the appropriate XCs to the LSP by referencing the L2VPN profile in the XC configuration. In the following example, the users maps three XCs to the the primary LSP tunnel by referencing the **troll1** profile in the configuration for those XCs:

```
[local]Redback#configure

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group delta

[local]Redback(config-l2vpn-xc-group)#xc 5/2 vpi-vci 5 2 vc-id 338
profile troll1

[local]Redback(config-l2vpn-xc-group)#xc-group troll

[local]Redback(config-l2vpn-xc-group)#xc 10/12 vlan-id 12 vc-id 335
profile troll1

[local]Redback(config-l2vpn-xc-group)#xc-group zzz

[local]Redback(config-l2vpn-xc-group)#xc 5/21 vpi-vci 5 2 vc-id 3386
profile troll1
```

3.15.3 Configuring an LSP to be Exclusive

The following example shows how to configure an LSP to be exclusive, as described in the *Configure an RSVP LSP* section in *Configuring MPLS*.

```
[local]Redback#configure

[local]Redback(config)#context local

[local]Redback(config-ctx)#router rsvp

[local]Redback(config-rsvp)#lsp lsp1

[local]Redback(config-rsvp-lsp)#exclusive
```

3.16 Example - L2VPN XC Redundancy

The following example shows how to configure master-slave mode L2VPN XC redundancy on three nodes in a hub-and-spoke network:

Configure the Hub node. First, create an L2VPN profile that configures the LSP tunnels to use for the primary and backup L2VPN XCs, the peer addresses of the spokes that will host the remote end of the primary and backup XCs, master-slave redundancy on associated XCs. Configure an SNMP trap to be generated when the L2VPN XC transitions from up, down, or standby status.

```
[local]Redback(config)#l2vpn profile foo

[local]Redback(config-l2vpn-xc-profile)#peer 100.100.100.1

[local]Redback(config-l2vpn-xc-profile-peer)#tunnel lsp lsp-to-target1

[local]Redback(config-l2vpn-xc-profile-peer)#redundancy-mode master-slave

[local]Redback(config-l2vpn-xc-profile-peer)#exit

[local]Redback(config-l2vpn-xc-profile)#backup peer 100.100.100.2

[local]Redback(config-l2vpn-xc-profile-peer)#tunnel lsp lsp-to-target2

[local]Redback(config-l2vpn-xc-profile-peer)#snmp trap

[local]Redback(config-l2vpn-xc-profile-peer)# #end
```

Attach the L2VPN profile to the primary XC, configure the XC for redundancy, and configure the backup XC:

```
[local]Redback#configure

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group default

[local]Redback(config-l2vpn-xc-group)#xc 10/3 vlan-id 100 vc-id 100
profile foo backup

[local]Redback(config-l2vpn-xc-prime]# vc-id 200 peer 100.100.100.2
```

Configure the spoke (slave) node that hosts the remote end of the primary XC. First, create an L2VPN profile that specifies the peer address of the host node, and the name of the LSP on which to configure the primary L2VPN XC:

```
[local]Redback(config)#l2vpn profile foo

[local]Redback(config-l2vpn-xc-profile)#peer 70.70.70.1

[local]Redback(config-l2vpn-xc-profile-peer)#tunnel lsp lsp-to-hub

[local]Redback(config-l2vpn-xc-profile-peer)#exit
```

Next, attach the profile to the primary L2VPN XC. Be aware that the VC ID on both ends of the primary XC must match.

```
[local]Redback#configure

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group default

[local]Redback(config-l2vpn-xc-group)#xc 5/6 vlan-id 100 vc-id 100
profile foo

[local]Redback(config-l2vpn-xc-group)#end
```

Configure the second spoke (slave) node that hosts the remote endpoint of the backup XC. First, create an L2VPN profile that specifies the peer address of the host node and the name of the LSP on which to configure the backup XC:

```
[local]Redback(config)#l2vpn profile foo

[local]Redback(config-l2vpn-xc-profile)#peer 70.70.70.1

[local]Redback(config-l2vpn-xc-profile-peer)#tunnel lsp lsp-to-hub

[local]Redback(config-l2vpn-xc-profile-peer)#exit
```

Next, attach the L2VPN profile to the backup XC. Be aware that the VC ID on both ends of the backup XC configuration must match:

```
[local]Redback#configure

[local]Redback(config)#context local

[local]Redback(config-ctx)#l2vpn

[local]Redback(config-l2vpn)#xc-group default

[local]Redback(config-l2vpn-xc-group)#xc 5/6 vlan-id 100 vc-id 200
profile foo

[local]Redback(config-l2vpn-xc-group)#end
```