



CHAPTER 5

Creating an L2VPN Policy

This chapter covers the basic steps to create an L2VPN policy. It contains the following sections:

- [Defining an L2VPN Policy, page 5-1](#)
- [Defining an Ethernet ERS \(EVPL\) Policy with a CE, page 5-3](#)
- [Defining an Ethernet ERS \(EVPL\) Policy without a CE, page 5-8](#)
- [Defining an Ethernet EWS \(EPL\) Policy with a CE, page 5-14](#)
- [Defining an Ethernet EWS \(EPL\) Policy without a CE, page 5-22](#)
- [Defining a Frame Relay Policy with a CE, page 5-28](#)
- [Defining a Frame Relay Policy without a CE, page 5-31](#)
- [Defining an ATM Policy with a CE, page 5-33](#)
- [Defining an ATM Policy without a CE, page 5-36](#)

Defining an L2VPN Policy

You must define an L2VPN policy before you can provision a Cisco IP Solution Center (ISC) service. An L2VPN policy defines the common characteristics shared by the end-to-end wire attributes and Attachment Circuit (AC) attributes.

A policy is a template of most of the parameters needed to define an L2VPN service request. After you define it, an L2VPN policy can be used by all the L2VPN service requests that share a common set of characteristics. You create a new L2VPN policy whenever you create a new type of service or a service with different parameters. L2VPN policy creation is normally performed by experienced network engineers.

A policy can be shared by one or more service requests that have similar service requirements. The Editable check box gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change to other valid values for the particular policy item. If the value is *not* set to editable, the service request creator cannot change the policy item.

The four major categories of an L2VPN policy correspond to the four major services that L2VPN provides:

- Point-to-point Ethernet Relay Service (ERS). The Metro Ethernet Forum (MEF) name for this service is Ethernet Virtual Private Line (EVPL). See [Layer 2 Terminology Conventions, page D-1](#) for more information about terms used to denote L2VPN services in this guide.
- Point-to-point Ethernet Wire Service (EWS). The MEF name for this service is Ethernet Private Line (EPL).

- Frame Relay over MPLS (FRoMPLS)
- ATM over MPLS (ATMoMPLS)

To define an L2VPN policy in ISC, perform the following steps.

Step 1 Choose **Service Design > Policies**.

The Policies window appears.

Step 2 Click **Create**.

Step 3 Choose **L2VPN (P2P) Policy**.

When you choose **L2VPN (P2P) Policy**, the L2VPN (Point to Point) Policy Creation window appears.

Step 4 Choose **L2VPN on MPLS Core**.

The window in [Figure 5-1](#) appears.

Figure 5-1 Creating an L2VPN Policy

The screenshot shows the 'L2VPN(Point To Point) Policy Editor' window. The breadcrumb trail is 'You Are Here: Service Design > Policies'. The 'Customer' field is set to 'None'. The form contains the following fields and values:

Attribute	Value
Policy Name *	[Empty text box]
Policy Owner:	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
Customer *	[Empty text box] <input type="button" value="Select"/>
Service Type:	<input checked="" type="radio"/> L2VPN ERS <input type="radio"/> L2VPN EWS <input type="radio"/> Frame Relay <input type="radio"/> ATM
CE Present:	<input checked="" type="checkbox"/>

Note: * - Required Field

Navigation buttons: < Back, Next >, Finish, Cancel

Step 5 Enter a **Policy Name** for the L2VPN policy.

Step 6 Choose the **Policy Owner** for the L2VPN policy.

There are three types of L2VPN policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this L2VPN policy.

This ownership has relevance when the ISC Role-Based Access Control (RBAC) comes into play. For example, an L2VPN policy that is customer-owned can only be seen by operators who are allowed to work on this customer-owned policy.

Similarly, operators who are allowed to work on a provider's network can view, use, and deploy a particular provider-owned policy.

Step 7 Click **Select** to choose the owner of the L2VPN.

(If you choose Global ownership, the Select function is not available.) The Select Customer window or the Select Provider window appears and you can choose an owner of the policy and click **Select**.

Step 8 Choose the **Service Type** of the L2VPN policy.

There are four service types for L2VPN policies:

- L2VPN ERS (EVPL)
- L2VPN EWS (EPL)
- Frame Relay
- ATM

Subsequent sections of this chapter cover setting up the policies for each of these services.

Step 9 Check the **CE Present** check box if you want ISC to ask the service operator who uses this L2VPN policy to provide a CE router and interface during service activation.

The default is CE present in the service.

If you do not check the **CE Present** check box, ISC asks the service operator, during service activation, only for the U-PE or the N-PE router and customer-facing interface.

Step 10 Click **Next**.

The next sections contain examples of setting policies for the service types, with and without a CE present.

Defining an Ethernet ERS (EVPL) Policy with a CE

This section describes defining an Ethernet ERS (EVPL) policy with CE present. [Figure 5-2](#) is an example of the first page of this policy.

Figure 5-2 Ethernet ERS (EVPL) Policy with a CE

L2VPN(Point To Point) Policy Editor

Attribute	Value
Policy Name *	l2vpnErsCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input checked="" type="radio"/> L2VPN ERS <input type="radio"/> L2VPN EWS <input type="radio"/> Frame Relay <input type="radio"/> ATM
CE Present:	<input checked="" type="checkbox"/>

Note: * - Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

138471

Perform the following steps.

Step 1 Click **Next**. The window in [Figure 5-3](#) appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-3 Ethernet ERS (EVPL) with CE Policy Attributes

Attribute	Value	Editable
PE Information		
Standard UNI Port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CE Information		
Interface Type	ANY	
Interface Format		
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Interface Type for UNI Display		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
VLAN and Other Information		
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VC ID AutoPick	<input checked="" type="checkbox"/>	
VLAN Name		
Use PseudoWireClass	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L2VPN Group Name		
E-Line Name		
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
Use Existing ACL Name		
Port-Based ACL Name		<input checked="" type="checkbox"/>
UNI MAC Addresses	0600.0CCC.CCCD(permit),0600.0CCC.CCCD(deny)	<input checked="" type="checkbox"/> Edit
UNI Port Security		
N-PE Pseudo-wire On SVI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Translation	<input checked="" type="radio"/> No <input type="radio"/> 1:1 <input type="radio"/> 2:1	<input checked="" type="checkbox"/>
PW Tunnel Selection	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: *. Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211688

Step 2 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.



Note

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.

Step 3 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a U-PE or N-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**

- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.



Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 8 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 9 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 10 Check the **VLAN ID AutoPick** check box if you want ISC to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 11 Check the **VC ID AutoPick** check box if you want ISC to choose a VC ID.

If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

Step 12 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.

Step 13 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in ISC. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes for IOS XR Devices, page 2-10](#) for additional information on pseudowire class support for IOS XR devices.

Step 14 Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 2-14](#).

Step 15 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the **p2p** name, ISC generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.

Step 16 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 17 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 18 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this box is unchecked and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 19 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note ISC does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 20 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 21 Choose a **UNI Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**



Note Enter a UNI Port Type only if the encapsulation type is DEFAULT.

- Step 22** Check the **UNI Port Security** check box (see [Figure 5-4](#)) if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
 - For **Aging**, enter the length of time the MAC address can stay on the port security table.
 - For **Violation Action**, choose what action will occur when a port security violation is detected:
 - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
 - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 5-4 UNI Port Security

UNI Port Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Maximum MAC Address	<input type="text"/> (1 - 8448)	<input checked="" type="checkbox"/>
Aging (in minutes)	<input type="text"/> (0 - 1440)	<input checked="" type="checkbox"/>
Violation Action	PROTECT <input type="button" value="v"/>	<input checked="" type="checkbox"/>
Secure MAC Addresses	<input type="text"/> <input type="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

- Step 23** Check the **Enable Storm Control** check box (see [Figure 5-5](#)) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 5-5 Enable Storm Control

Enable Storm Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UNI Storm Control		
Unicast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Broadcast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Multicast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>

138440

- Step 24** Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.

This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.

**Note**

The **N-PE Pseudo-wire on SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 25 Specify the type of **VLAN Translation** for this policy by clicking the appropriate radio button.

The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation.
- **2:1**—2:1 VLAN translation.

**Note**

For detailed coverage of setting up VLAN translation, see [Appendix C, “Setting Up VLAN Translation.”](#)

Step 26 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.

**Note**

The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 27 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files”](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 28 Click **Finish**.

Defining an Ethernet ERS (EVPL) Policy without a CE

This section describes defining an Ethernet ERS (EVPL) policy without a CE present. [Figure 5-6](#) is an example of the first page of this policy.

Figure 5-6 Ethernet ERS (EVPL) Policy without a CE

Attribute	Value
Policy Name *	L2vpnErsNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input checked="" type="radio"/> L2VPN ERS <input type="radio"/> L2VPN EWS <input type="radio"/> Frame Relay <input type="radio"/> ATM
CE Present:	<input type="checkbox"/>

Note: *- Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

138472

Perform the following steps.

Step 1 Click **Next**. The window in [Figure 5-7](#) appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-7 Ethernet ERS (EVPL) without CE Policy Attributes

L2VPN(Point To Point) Policy Editor

Attribute	Value	Editable
N-PE/U-PE Information		
Interface Type	ANY	
Standard UNI Port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Interface Format		
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Interface Type for UNI Display		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
VLAN and Other Information		
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VC ID AutoPick	<input checked="" type="checkbox"/>	
VLAN Name		
Use PseudoWireClass	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L2VPN Group Name		
E-Line Name		
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
Use Existing ACL Name		
Port-Based ACL Name		<input checked="" type="checkbox"/>
UNI MAC Addresses	0600.00CC.0CCD(permit),0600.00CC.0CCD(deny) Edit	<input checked="" type="checkbox"/>
UNI Port Security		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
N-PE Pseudo-wire On SVI		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Translation		
	<input checked="" type="radio"/> No <input type="radio"/> 1:1 <input type="radio"/> 2:1	<input checked="" type="checkbox"/>
PW Tunnel Selection		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: * - Required Field

- Step 2 of 3 -

[< Back](#) [Next >](#) [Finish](#) [Cancel](#)

211688

Step 2 Choose a N-PE/U-PE **Interface Type** from the drop-down list.

You can choose a particular interface as a CE, N-PE, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 3 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

**Note**

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.

Step 4 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

**Note**

If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 8 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 9 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 10 Check the **VLAN ID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 11 Check the **VC ID AutoPick** check box if you want ISC to choose a VC ID.

If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

Step 12 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in ISC. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes for IOS XR Devices, page 2-10](#) for additional information on pseudowire class support for IOS XR devices.

Step 13 Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 2-14](#).

Step 14 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, ISC generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A----6503-B). If the default name is more than 32 characters, the device names are truncated.

Step 15 Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.

Step 16 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 17 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 18 Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is unchecked and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

Step 19 Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note ISC does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 20 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you unchecked the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 21 Choose a **UNI Port Type**.

The choices are:

- **Access Port**
- **Trunk with Native VLAN**



Note Enter a UNI Port Type only if the encapsulation type is DEFAULT.

- Step 22** Check the **UNI Port Security** check box (see [Figure 5-8](#)) if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
 - For **Aging**, enter the length of time the MAC address can stay on the port security table.
 - For **Violation Action**, choose what action will occur when a port security violation is detected:
 - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
 - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 5-8 UNI Port Security

UNI Port Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Maximum MAC Address	<input type="text"/> (1 - 8448)	<input checked="" type="checkbox"/>
Aging (in minutes)	<input type="text"/> (0 - 1440)	<input checked="" type="checkbox"/>
Violation Action	PROTECT <input type="button" value="v"/>	<input checked="" type="checkbox"/>
Secure MAC Addresses	<input type="text"/> <input type="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

- Step 23** Check the **Enable Storm Control** check box (see [Figure 5-9](#)) to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.

Figure 5-9 Enable Storm Control

Enable Storm Control	<input checked="" type="checkbox"/>	
UNI Storm Control		
Unicast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Broadcast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Multicast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>

138440

- Step 24** Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.

This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.



Note

The **N-PE Pseudo-wire On SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 25 Specify the type of **VLAN Translation** for this policy by clicking the appropriate radio button.

The choices are:

- **No**—No VLAN translation is performed. (This is the default.)
- **1:1**—1:1 VLAN translation.
- **2:1**—2:1 VLAN translation.



Note For detailed coverage of setting up VLAN translation, see [Appendix C, “Setting Up VLAN Translation.”](#)

Step 26 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.



Note The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 27 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files”](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 28 Click **Finish**.

Defining an Ethernet EWS (EPL) Policy with a CE

This section describes defining an Ethernet EWS (EPL) policy with CE present. [Figure 5-10](#) is an example of the first page of this policy.

Figure 5-10 Ethernet EWS (EPL) Policy with a CE

L2VPN(Point To Point) Policy Editor

Attribute	Value
Policy Name *	L2vpnEwsCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input type="radio"/> L2VPN ERS <input checked="" type="radio"/> L2VPN EWS <input type="radio"/> Frame Relay <input type="radio"/> ATM
CE Present:	<input checked="" type="checkbox"/>

Note: *- Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

138473

Perform the following steps.

Step 1 Click **Next**. The window in [Figure 5-11](#) appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-11 Ethernet EWS (EPL) with CE Policy Attributes

L2VPN(Point To Point) Policy Editor

Attribute	Value	Editable
PE Information		
Standard UNI Port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CE Information		
Interface Type	ANY	
Interface Format		
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Interface Type for UNI Display		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
VLAN and Other Information		
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VC ID AutoPick	<input checked="" type="checkbox"/>	
VLAN Name		
Use PseudoWireClass	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L2VPN Group Name		
E-Line Name		
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
Use Existing ACL Name		
Port-Based ACL Name		<input checked="" type="checkbox"/>
UNI MAC Addresses	0600.0CCC.CCCD(permit),0600.0CCC.CCCD(deny)	<input checked="" type="checkbox"/> Edit
UNI Port Security	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Protocol Tunnelling	<input type="checkbox"/>	<input checked="" type="checkbox"/>
N-PE Pseudo-wire On SWI	<input type="checkbox"/>	<input checked="" type="checkbox"/>
MTU size		<input checked="" type="checkbox"/> (1500-9216)
PW Tunnel Selection	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: *- Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211690

Step 2 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.



Note

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.



Note

In previous releases, the only Layer 2 VPN support for EWS (EPL) was from EWS (EPL) to EWS (EPL). In ISC 4.1.2 and later, support is also from EWS (EPL) to Network to Network Interface (NNI) as a trunk port. To create this new type of service request, you need to create an EWS (EPL) “hybrid” policy by unchecking the standard UNI flag. When using the EWS (EPL) hybrid policy for service request creation, check the **Standard UNI Port flag** for the EWS (EPL) side of the connection and uncheck the standard UNI flag for the NNI side of the connection.



Note

In the case of hybrid services, UNI on an N-PE running IOS XR is not supported.

Step 3 Choose an **Interface Type** from the drop-down list.

You can choose a particular interface on a U-PE or N-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.



Note

If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Check the **Keep Alive** check box to configure keepalives on the UNI port.


By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 8 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

Step 9 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is checked by default.

- Step 10** Check the **VLAN ID AutoPick** check box if you want ISC to choose a VLAN ID.
If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.
- Step 11** Check the **VC ID AutoPick** check box if you want ISC to choose a VC ID.
If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.
- Step 12** Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.
This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in ISC. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes for IOS XR Devices, page 2-10](#) for additional information on pseudowire class support for IOS XR devices.
- Step 13** Choose an **L2VPN Group Name** from the drop-down list.
The choices are:
- **ISC**
 - **VPNSC**
- This attribute is used for provisioning the L2VPN group name on IOS XR devices.
-
-  **Note** The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 2-14](#).
-
- Step 14** Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.
This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, ISC generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.
- Step 15** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.
The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.
- Step 16** Check the **VLAN ID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.
- Step 17** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 18** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 19** Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this check box is not checked and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).
- Step 20** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note ISC does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

Step 21 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

Step 22 Check the **UNI Port Security** check box (see [Figure 5-12](#)) if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

- a. For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
- b. For **Aging**, enter the length of time the MAC address can stay on the port security table.
- c. For **Violation Action**, choose what action will occur when a port security violation is detected:
 - **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - **SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
- d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 5-12 UNI Port Security




UNI Port Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Maximum MAC Address	<input type="text"/> (1 - 8448)	<input checked="" type="checkbox"/>
Aging (in minutes)	<input type="text"/> (0 - 1440)	<input checked="" type="checkbox"/>
Violation Action	PROTECT <input type="button" value="v"/>	<input checked="" type="checkbox"/>
Secure MAC Addresses	<input type="text"/> <input type="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

Step 23 Check the **Enable Storm Control** check box (see [Figure 5-13](#)) to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm. Enter a threshold value for each type of traffic.

The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.




Figure 5-13 Enable Storm Control

Enable Storm Control	<input checked="" type="checkbox"/>	
UNI Storm Control		
Unicast Traffic(0.0 - 100.0%) 	<input type="text"/>	<input checked="" type="checkbox"/>
Broadcast Traffic(0.0 - 100.0%) 	<input type="text"/>	<input checked="" type="checkbox"/>
Multicast Traffic(0.0 - 100.0%) 	<input type="text"/>	<input checked="" type="checkbox"/>

138440

Step 24 Check the **Protocol Tunnelling** check box (see Figure 5-14) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 5-14 Protocol Tunnelling

Protocol Tunnelling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enable cdp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cdp shutdown threshold	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
cdp drop threshold 	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
Enable vtp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
vtp shutdown threshold	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
vtp drop threshold 	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
Enable stp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
stp shutdown threshold	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
stp drop threshold 	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
Recovery Interval (in seconds)	<input type="text"/> (30-86400)	<input type="checkbox"/>

138368

For each protocol that you choose, enter the shutdown threshold and drop threshold for that protocol:

- Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- cdp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
- Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
- Enable stp**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- stp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
- Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 25 Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.

This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.

**Note**

The **N-PE Pseudo-wire On SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 26 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. ISC does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In ISC 5.1, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, ISC 5.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

Step 27 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.

**Note**

The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 28 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files”](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 29 Click **Finish**.

Defining an Ethernet EWS (EPL) Policy without a CE

This section describes how to define an Ethernet EWS (EPL) policy without a CE present. [Figure 5-15](#) is an example of the first page of this policy.

Figure 5-15 Ethernet EWS (EPL) Policy without a CE

The screenshot shows the 'L2VPN(Point To Point) Policy Editor' window. It contains a table with two columns: 'Attribute' and 'Value'. The 'Policy Name' attribute is set to 'L2vpnEwsNoCe'. The 'Policy Owner' attribute has three radio button options: 'Customer', 'Provider', and 'Global Policy', with 'Global Policy' selected. The 'Service Type' attribute has four radio button options: 'L2VPN ERS', 'L2VPN EWS', 'Frame Relay', and 'ATM', with 'L2VPN EWS' selected. The 'CE Present' attribute has a checkbox that is currently unchecked. Below the table, there is a note: 'Note: * - Required Field'. At the bottom of the window, there are navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The status bar at the bottom left indicates '- Step 1 of 2 -'.

Attribute	Value
Policy Name *	L2vpnEwsNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input type="radio"/> L2VPN ERS <input checked="" type="radio"/> L2VPN EWS <input type="radio"/> Frame Relay <input type="radio"/> ATM
CE Present:	<input type="checkbox"/>

Note: * - Required Field

- Step 1 of 2 -

Perform the following steps.

Step 1 Click **Next**. The window in [Figure 5-16](#) appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-16 Ethernet EWS (EPL) without CE Policy Attributes

L2VPN(Point To Point) Policy Editor

Attribute	Value	Editable
N-PE/U-PE Information		
Interface Type	ANY	
Standard UNI Port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Interface Format		
UNI Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Interface Type for UNI Display		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
VLAN and Other Information		
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VC ID AutoPick	<input checked="" type="checkbox"/>	
VLAN Name		
Use PseudoWireClass	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L2VPN Group Name	ISC	
E-Line Name		
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
Use Existing ACL Name		
Port-Based ACL Name		<input checked="" type="checkbox"/>
UNI MAC Addresses	0600.0CCC.CCCD(permit),0600.0CCC.CCCD(deny)	<input checked="" type="checkbox"/> Edit
UNI Port Security		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Protocol Tunnelling		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
N-PE Pseudo-wire On SVI		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
MTU size		
		<input checked="" type="checkbox"/> (1500-9216)
PW Tunnel Selection		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: *, Required Field

Step 2 of 3 -

< Back Next > Finish Cancel

204777

Step 2 Choose a N-PE/U-PE **Interface Type** from the drop-down list.

You can choose a particular interface as a CE, N-PE, or U-PE interface based on the service provider's POP design. The interfaces are:

- **ANY** (Any interface can be chosen.)
- **Port-Channel** (A bundle of ports that share the same characteristics—this gives the service provider the ability to aggregate bandwidth and protection.)
- **Ethernet**
- **FastEthernet**
- **GE-WAN**
- **GigabitEthernet**
- **TenGigabitEthernet**
- **TenGigE**

The value defined here functions as a filter to restrict the interface types an operator can see during L2VPN service request creation.

Step 3 Check the **Standard UNI Port** check box to enable port security.

This is the default. When you uncheck the check box, the port is treated as an uplink with no security features, and the window dynamically changes to eliminate items related to port security.

**Note**

The **Standard UNI Port** attribute will be unavailable within service requests based on this policy if the UNI is on an N-PE device running IOS XR.

**Note**

In previous releases, the only Layer 2 VPN support for EWS (EPL) was from EWS (EPL) to EWS (EPL). In ISC 4.1.2 and later, support is also from EWS (EPL) to Network to Network Interface (NNI) as a trunk port. To create this new type of service request, you need to create an EWS (EPL) “hybrid” policy by unchecking the standard UNI flag. When using the EWS (EPL) hybrid policy for service request creation, check the **Standard UNI Port flag** for the EWS (EPL) side of the connection and uncheck the standard UNI flag for the NNI side of the connection.

**Note**

In the case of hybrid services, UNI on an N-PE running IOS XR is not supported.

Step 4 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface’s slot/port location on all or most of the network devices in the service.

Step 5 Choose an **Encapsulation** type.

The choices are:

- **DOT1Q**
- **DEFAULT**

If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.

**Note**

If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Check the **Keep Alive** check box to configure keepalives on the UNI port.

By default, this check box is unchecked, which causes the command **no keepalive** to be provisioned on the UNI port. This prevents a CPE from sending keepalive packets to the U-PE, for security purposes. This attribute is editable to support modification on a per-service request basis.

Step 8 Check the **ANY** check box to display all interface types as choices for the UNI interface (when creating service requests based on this policy).

This check box is not checked by default.

Step 9 Check the **UNI** check box to display all interfaces defined as type UNI as choices for the UNI interface (when creating service requests based on this policy).

This check box is not checked by default.

Step 10 Check the **VLAN ID AutoPick** check box if you want ISC to choose a VLAN ID.

If you do not check this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 11 Check the **VC ID AutoPick** check box if you want ISC to choose a VC ID.

If you do not check this check box, you will be prompted to provide the VC ID in a VC ID field during service activation.

- Step 12** Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in ISC. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes for IOS XR Devices, page 2-10](#) for additional information on pseudowire class support for IOS XR devices.

- Step 13** Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 2-14](#).

- Step 14** Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, ISC generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.

- Step 15** Enter a **VLAN NAME** (optional) to specify a name to describe the VLAN.

The name must be one token (no spaces allowed.) The limit for the VLAN name is 32 characters. The name has to be unique.

- Step 16** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

- Step 17** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

- Step 18** Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port.

By default, this check box is not checked and ISC automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

- Step 19** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



Note ISC does not create this ACL automatically. The ACL must already exist on the device, or be added as part of a template, before the service request is deployed. Otherwise, deployment will fail.

- Step 20** Enter one or more Ethernet MAC addresses in **UNI MAC addresses**.

This selection is present only if you uncheck the **Use Existing ACL Name** check box. Click the **Edit** button to bring up a pop-up window in which you enter MAC addresses to be allowed or denied on the port. You can also specify a range of addresses by setting a base MAC address and a filtered MAC address.

- Step 21** Check the **UNI Port Security** check box (see [Figure 5-4](#)) if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
 - For **Aging**, enter the length of time the MAC address can stay on the port security table.
 - For **Violation Action**, choose what action will occur when a port security violation is detected:
 - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
 - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
 - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
 - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 5-17 UNI Port Security

UNI Port Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Maximum MAC Address	<input type="text"/> (1 - 8448)	<input checked="" type="checkbox"/>
Aging (in minutes)	<input type="text"/> (0 - 1440)	<input checked="" type="checkbox"/>
Violation Action	PROTECT <input type="button" value="v"/>	<input checked="" type="checkbox"/>
Secure MAC Addresses	<input type="text"/> <input type="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

- Step 22** Check the **Enable Storm Control** check box (see [Figure 5-18](#)) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm.

Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, further traffic of that type is suppressed until the incoming traffic falls below the threshold level.




Figure 5-18 Enable Storm Control

Enable Storm Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UNI Storm Control		
Unicast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Broadcast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Multicast Traffic(0.0 - 100.0%) <input type="button" value="i"/>	<input type="text"/>	<input checked="" type="checkbox"/>

138440

- Step 23** Check the **Protocol Tunneling** check box (see [Figure 5-14](#)) if you want to define the Layer 2 Bridge Protocol Data Unit (BPDU) frames that can be tunneled over the core to the other end.

Figure 5-19 Protocol Tunnelling

Protocol Tunnelling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enable cdp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
cdp shutdown threshold	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
cdp drop threshold 	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
Enable vtp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
vtp shutdown threshold	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
vtp drop threshold 	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
Enable stp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
stp shutdown threshold	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
stp drop threshold 	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
Recovery Interval (in seconds)	<input type="text"/> (30-86400)	<input type="checkbox"/>

138368

For each protocol that you check, enter the shutdown threshold and drop threshold for that protocol:

- a. **Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- b. **cdp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.
- d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.
- g. **Enable stp**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **stp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.
- i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
- j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 24 Check the **N-PE Pseudo-wire On SVI** check box to configure the pseudowire connection on the switched virtual interface of the OSM card.

This check box is checked by default. If the check box is not checked, the pseudowire will be provisioned on the subinterface of the PFC card, if it is available. This option is only available for C76xx devices.

**Note**

The **N-PE Pseudo-wire On SVI** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 25 Enter the **MTU Size** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. ISC does not perform an integrity check for this customized value. If a service request goes to the Failed Deploy state because this size is not accepted, you must adjust the size until the Service Request is deployed.

In ISC 5.1, different platforms support different ranges.

- For the 3750 and 3550 platforms, the MTU range is 1500-1546.
- For the 7600 ethernet port, the MTU size is always 9216. Even with the same platform and same IOS release, different line cards support the MTU differently. For example, older line cards only take an MTU size of 9216 and newer cards support 1500-9216. However, ISC 5.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

Step 26 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.



Note

The **PW Tunnel Selection** attribute will be unavailable within service requests based on this policy for devices running IOS XR.

Step 27 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files”](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 28 Click **Finish**.

Defining a Frame Relay Policy with a CE

This section describes how to define a Frame Relay policy with CE present. [Figure 5-20](#) is an example of the first page of this policy.



Note

Frame Relay policies are not supported for devices running IOS XR.

Figure 5-20 Frame Relay Policy with a CE

L2VPN(Point To Point) Policy Editor

Attribute	Value
Policy Name *	FrameRelayCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input type="radio"/> L2VPN ERS <input type="radio"/> L2VPN EWS <input checked="" type="radio"/> Frame Relay <input type="radio"/> ATM
CE Present:	<input checked="" type="checkbox"/>

Note: *- Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

138484

Perform the following steps.

Step 1 Click **Next**. The window in [Figure 5-21](#) appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-21 Frame Relay with CE Policy Attributes

L2VPN(Point To Point) Policy Editor

Attribute	Value	Editable
PE Information		
CE Information		
Interface Type	ANY	
Interface Format		
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PW Tunnel Selection	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: *- Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211692

Step 2 Choose the **Interface Type** for the **CE** from the drop-down list.

The choices are:

- ANY
- Serial
- MFR

- POS
- Hssi
- BRI

Step 3 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, 1/0 indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose the CE Encapsulation type.

The choices are:

- FRAME RELAY
- FRAME RELAY IETF



Note

If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 5 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 6 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.

Step 7 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, "Working with Templates and Data Files"](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 8 Click **Finish**.

Defining a Frame Relay Policy without a CE

This section describes how to define a Frame Relay policy without a CE present. [Figure 5-22](#) is an example of the first page of this policy.

Figure 5-22 Frame Relay Policy without a CE

Attribute	Value
Policy Name *	FrameRelayNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input type="radio"/> L2VPN ERS <input type="radio"/> L2VPN EWS <input checked="" type="radio"/> Frame Relay <input type="radio"/> ATM
CE Present:	<input type="checkbox"/>

Note: *- Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

Perform the following steps.

Step 1 Click **Next**. The window in [Figure 5-23](#) appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-23 Frame Relay without CE Policy Attributes

Attribute	Value	Editable
N-PE/U-PE Information		
Interface Type	ANY	
Interface Format		
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
PW Tunnel Selection	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: *- Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

Step 2 Choose the N-PE/U-PE **Interface Type** for the CE from the drop-down list.

The choices are:

- ANY
- Serial
- MFR
- POS
- Hssi
- BRI

Step 3 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, 1/0 indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 4 Choose the N-PE/U-PE **Encapsulation** type.

The choices are:

- FRAME RELAY
- FRAME RELAY IETF



Note

If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 5 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 6 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.

Step 7 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, "Working with Templates and Data Files"](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 8 Click **Finish**.

Defining an ATM Policy with a CE

This section describes how to define an ATM policy with CE present. Figure 5-24 is an example of the first page of this policy.

Figure 5-24 ATM Policy with a CE

Attribute	Value
Policy Name *	AtmCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input type="radio"/> L2VPN ERS <input type="radio"/> L2VPN EWS <input type="radio"/> Frame Relay <input checked="" type="radio"/> ATM
CE Present:	<input checked="" type="checkbox"/>

Note: * - Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

Perform the following steps.

Step 1 Click **Next**. The window in Figure 5-25 appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-25 ATM with CE Policy Attributes

Attribute	Value	Editable
PE Information		
Transport Mode	VP	<input checked="" type="checkbox"/>
CE Information		
Interface Type	ANY	<input checked="" type="checkbox"/>
Interface Format		<input checked="" type="checkbox"/>
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use PseudoWireClass	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L2VPN Group Name		<input checked="" type="checkbox"/>
E-Line Name		<input checked="" type="checkbox"/>
PW Tunnel Selection		
PW Tunnel Selection	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: * - Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

Step 2 Choose the **Transport Mode** from the drop-down list.

The choices are:

- **VP**—Virtual path mode. This is the default.
- **VC**—Virtual circuit mode.
- **PORT**—Port mode. (Only supported for the IOS XR 3.7 platform.)



Note If you choose **PORT** as the transport mode, the attributes **ATM VCD/Sub-interface #** and **ATM VPI** will be disabled in the Link Attributes window of the service request based on this policy.

Step 3 Choose the **CE Interface Type** from the drop-down list.

The choices are:

- **ANY**
- **ATM**
- **Switch**

Step 4 Enter an **Interface Format** as the slot number/port number for the CE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose a **CE Encapsulation**.

The choices are:

- **AAL5SNAP**
- **AAL5MUX**
- **AAL5NLPID**
- **AAL2**



Note If the Interface Type is ANY, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in ISC. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes for IOS XR Devices, page 2-10](#) for additional information on pseudowire class support for IOS XR devices.

Step 8 Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 2-14](#).

Step 9 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, ISC generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.

Step 10 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default

Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.

Step 11 Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files”](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

Step 12 Click **Finish**.

Defining an ATM Policy without a CE

This section describes how to define an ATM policy without a CE present. [Figure 5-26](#) is an example of the first page of this policy.

Figure 5-26 ATM Policy without a CE

Attribute	Value
Policy Name *	AtmNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Service Type:	<input type="radio"/> L2VPN ERS <input type="radio"/> L2VPN EWS <input type="radio"/> Frame Relay <input checked="" type="radio"/> ATM
CE Present:	<input type="checkbox"/>

Note: *. Required Field

- Step 1 of 2 -

< Back Next > Finish Cancel

Perform the following steps.

Step 1 Click **Next**. The window in [Figure 5-27](#) appears.

The **Editable** check box gives you the option of making a field editable. If you check the **Editable** check box, the service operator who is using this L2VPN policy can modify the editable parameter during L2VPN service request creation.

Figure 5-27 ATM without CE Policy Attributes

Attribute	Value	Editable
N-PE/U-PE Information		
Transport Mode	VP	<input checked="" type="checkbox"/>
Interface Type	ANY	<input checked="" type="checkbox"/>
Interface Format		<input checked="" type="checkbox"/>
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use PseudoWireClass	<input type="checkbox"/>	<input checked="" type="checkbox"/>
L2VPN Group Name		<input checked="" type="checkbox"/>
E-Line Name		<input checked="" type="checkbox"/>
PW Tunnel Selection		
PW Tunnel Selection	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: *. Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

Step 2 Choose the **Transport Mode** from the drop-down list.

The choices are:

- **VP**—Virtual path mode. This is the default.
- **VC**—Virtual circuit mode.
- **PORT**—Port mode. (Only supported for the IOS XR 3.7 platform.)



Note If you choose **PORT** as the transport mode, the attributes **ATM VCD/Sub-interface #** and **ATM VPI** will be disabled in the Link Attributes window of the service request based on this policy.

Step 3 Choose the **N-PE/U-PE Interface Type** from the drop-down list.

The choices are:

- **ANY**
- **ATM**
- **Switch**

Step 4 Enter an **Interface Format** as the slot number/port number for the PE interface (for example, **1/0** indicates that the interface is located at slot 1, port 0).

This is especially useful to specify here if you know that the link will always go through a particular interface's slot/port location on all or most of the network devices in the service.

Step 5 Choose a **PE Encapsulation**.

The choices are:

- **AAL5**
- **AAL0**



Note If the Interface Type is **ANY**, ISC will not ask for an **Encapsulation** type in the policy.

Step 6 Check the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

Step 7 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is only applicable for IOS XR devices. If the check box is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in ISC. The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See [Creating and Modifying Pseudowire Classes for IOS XR Devices, page 2-10](#) for additional information on pseudowire class support for IOS XR devices.

Step 8 Choose an **L2VPN Group Name** from the drop-down list.

The choices are:

- **ISC**
- **VPNSC**

This attribute is used for provisioning the L2VPN group name on IOS XR devices.



Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see [Defining L2VPN Group Names for IOS XR Devices, page 2-14](#).

- Step 9** Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.
- This attribute is only applicable for IOS XR devices. If no value is specified for the p2p name, ISC generates a default name consisting of the names of the two PEs forming the pseudowire, separated by hyphens (for example, 6503-A---6503-B). If the default name is more than 32 characters, the device names are truncated.
- Step 10** Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.
- This attribute is unchecked by default
- Subsequently, when you create a service request based on this policy, you must specify the TE tunnel ID in a field provided. ISC uses the tunnel information to create and provision a pseudowire class that describes the pseudowire connection between two N-PEs. This pseudowire class can be shared by more than one pseudowire, as long as the pseudowires share the same tunnel ID and remote loopback address. You are responsible to ensure that the tunnel interface and associated ID are configured. During service request creation when you specify the tunnel ID number, ISC does not check the validity of the value. That is, ISC does not verify the existence of the tunnel.
- Step 11** Click the **Next** button, if you want to enable template support for the policy.
- The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix B, “Working with Templates and Data Files”](#). When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.
- Step 12** Click **Finish**.
-