Creating an L2VPN Policy

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

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.

Note If you are defining an L2TPv3 policy, seeChapter 6, “Creating an L2TPv3 Policy.”

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)
- Point-to-point Ethernet Wire Service (EWS)
- Frame Relay over MPLS (FRoMPLS)
- ATM over MPLS (ATMoMPLS)

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.

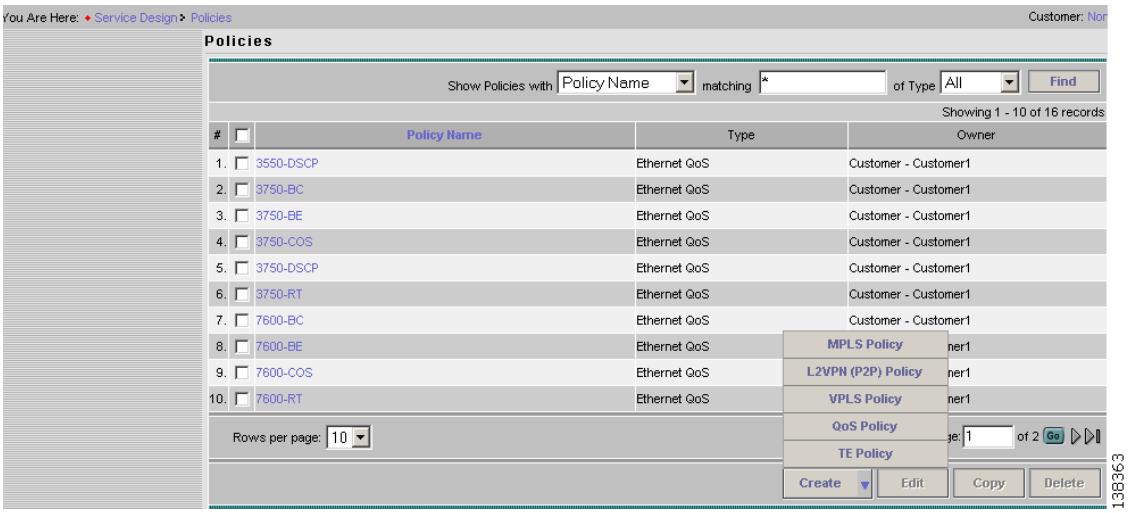
You create a new L2VPN policy whenever you create a new type of service or a service with different parameters. L2VPN policy creation is normally performed by experienced network engineers.

To define an L2VPN policy in ISC, use the following steps. See Figure 4-1.

Step 1 Select **Service Design** > **Policies**. The Policies window appears as shown in Figure 4-1.

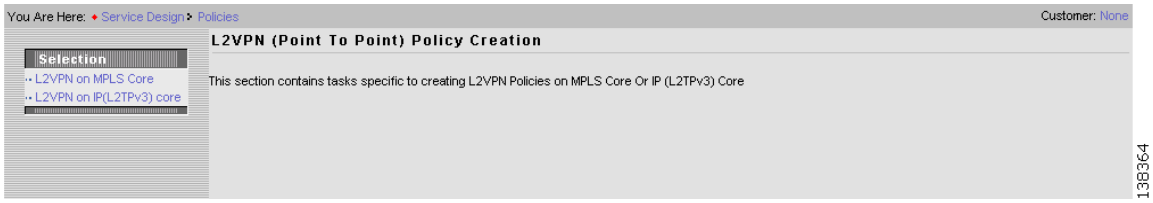
Step 2 Click **Create**.

Figure 4-1 Creating an L2VPN Policy



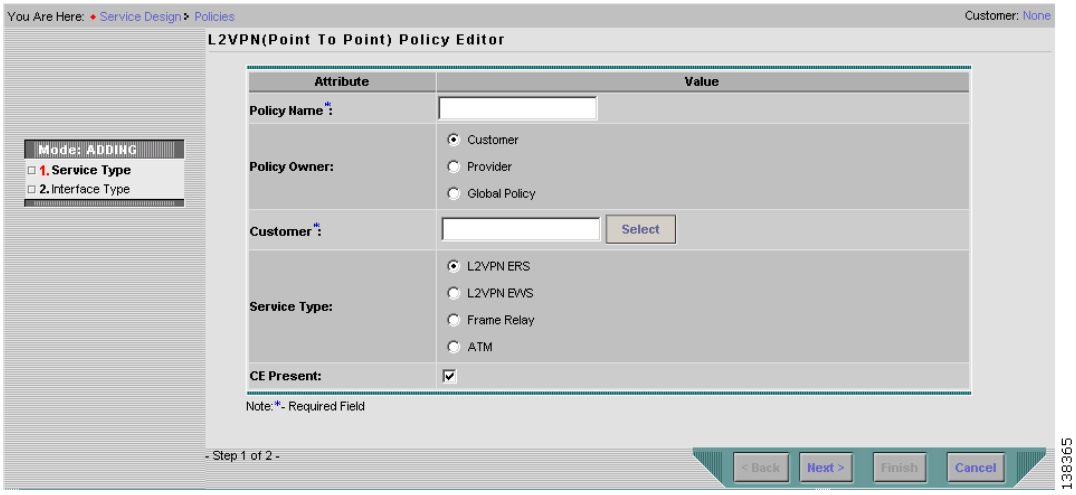
Step 3 Select **L2VPN (P2P) Policy**. When you select **L2VPN (P2P) Policy**, the window in Figure 4-3 appears.

Figure 4-2 Choosing a Policy Type



Step 4 Select **L2VPN on MPLS Core**. The window in Figure 4-3 appears.

Figure 4-3 Creating an L2VPN Policy



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
- L2VPN EWS
- Frame Relay
- ATM

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

Step 9 Select 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 select 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.

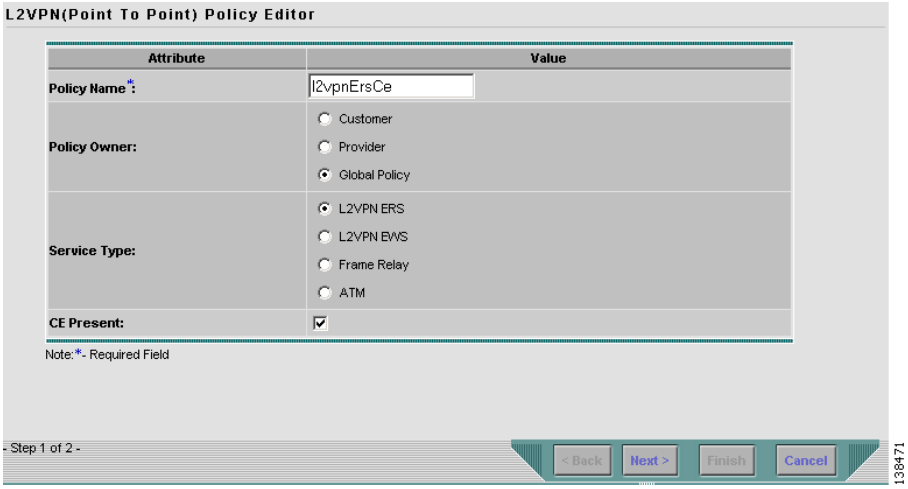
Step 10 Click **Next**.

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

Defining an Ethernet ERS Policy with a CE

This section describes defining an Ethernet ERS policy with CE present. Figure 4-4 is an example of the first page of this policy.

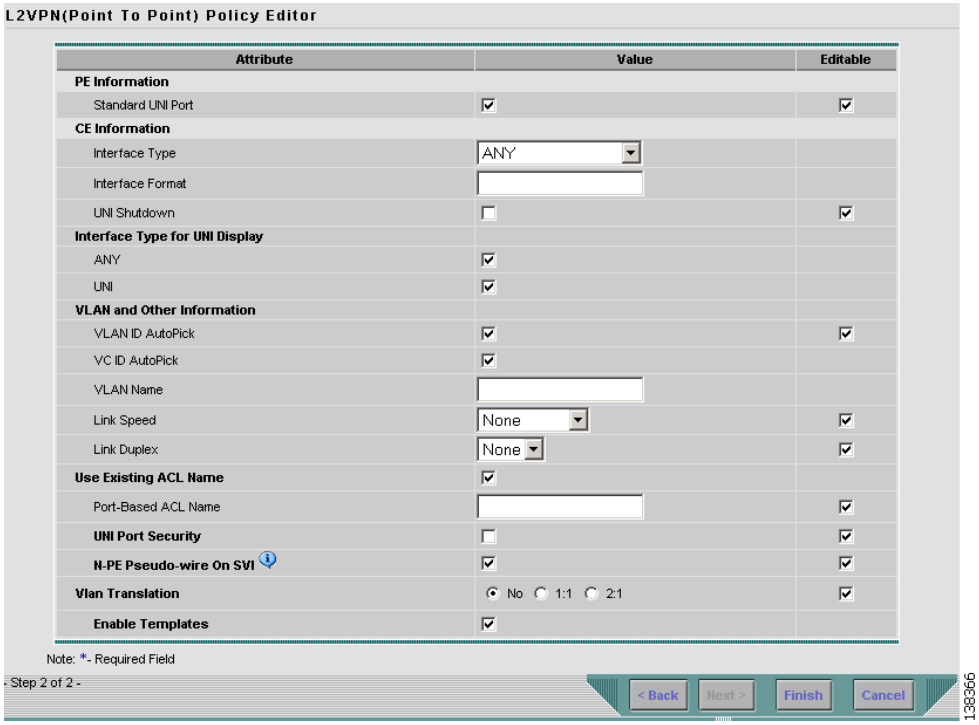
Figure 4-4 Ethernet ERS Policy with a CE



Step 1 Click **Next**. The window in Figure 4-5 appears.

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

Figure 4-5 Ethernet ERS with CE Policy Attributes



Step 2 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect 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.

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

You can choose to select 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**

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 policy.

Step 6 Select 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 Select 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 selected by default.

Step 8 Select 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 selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

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

Step 11 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. Two VLANs cannot share the same name.

Step 12 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 13 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 14 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this box is unselected 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 15 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect 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 17 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 18 Enter one or more Ethernet MAC addresses in **UNI MAC Addresses**.

Step 19 Select the **UNI Port Security** check box (see Figure 4-6) if you to 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:

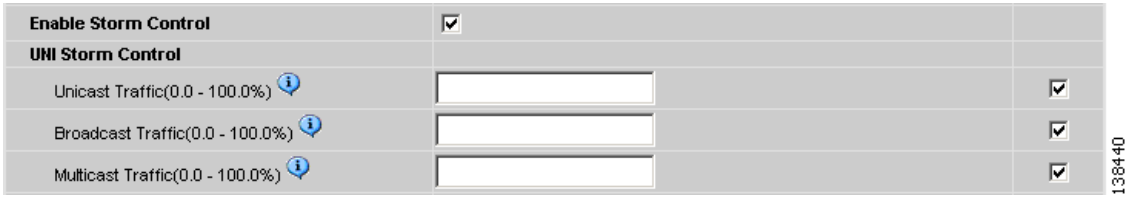
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value 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 4-6 UNI Port Security

Step 20 Select the **Enable Storm Control** check box (see Figure 4-7) 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 4-7 Enable Storm Control



Step 21 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If the check box is not selected, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 22 Specify the type of **VLAN Translation** for this policy by selecting 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 A, "Setting Up VLAN Translation."

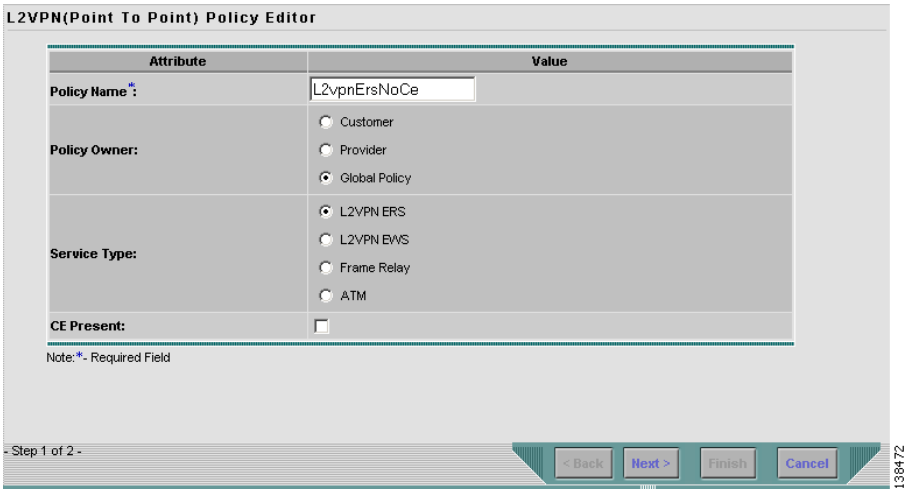
Step 23 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 24 Click **Finish**.

Defining an Ethernet ERS Policy without a CE

This section describes defining an Ethernet ERS policy with out a CE present. Figure 4-6 is an example of the first page of this policy.

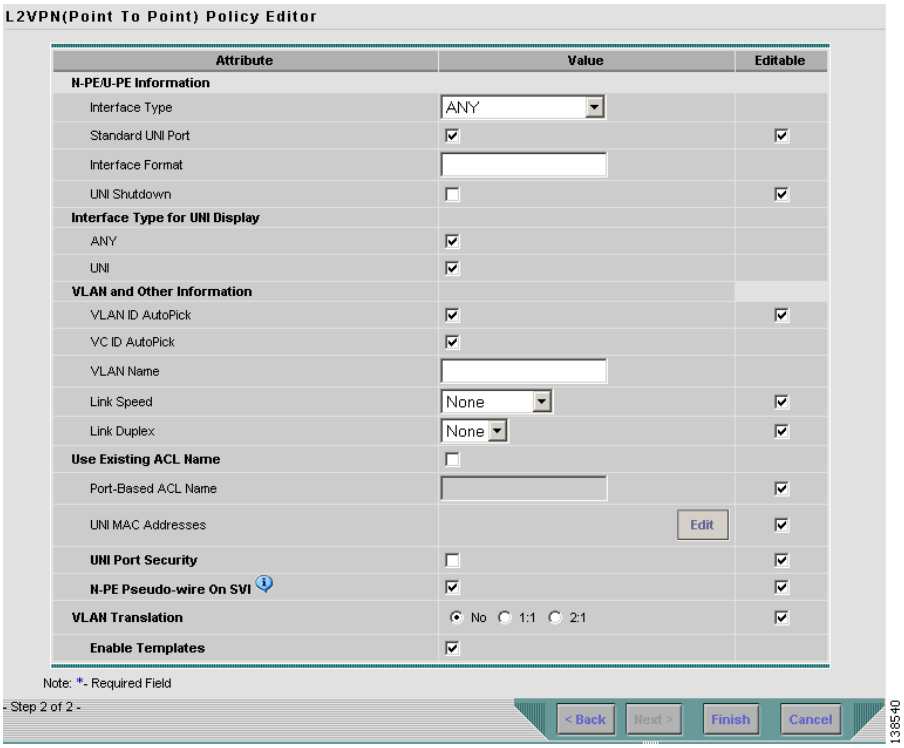
Figure 4-8 Ethernet ERS Policy without a CE



Step 1 Click **Next**. The window in Figure 4-9 appears.

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

Figure 4-9 Ethernet ERS without CE Policy Attributes



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

You can choose to select 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**

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

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect 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.

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 policy.

Step 6 Select 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 Select 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 selected by default.

Step 8 Select 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 selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

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

Step 11 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. Two VLANs cannot share the same name.

Step 12 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 13 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 14 Select 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 unselected 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 15 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect 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 17 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 18 Enter one or more Ethernet MAC addresses in **UNI MAC Addresses**.

Step 19 Select the **UNI Port Security** check box (see Figure 4-10) if you to 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:

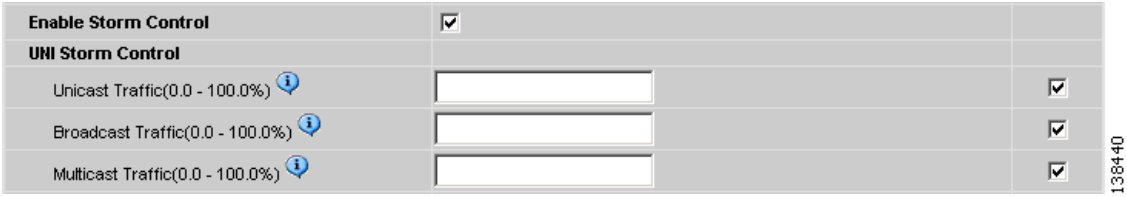
- **PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
- **RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value 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 4-10 UNI Port Security

Step 20 Select the **Enable Storm Control** check box (see Figure 4-11) 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 4-11 Enable Storm Control



Step 21 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If you deselect the check box, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 22 Specify the type of **VLAN Translation** for this policy by selecting 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 A, "Setting Up VLAN Translation."

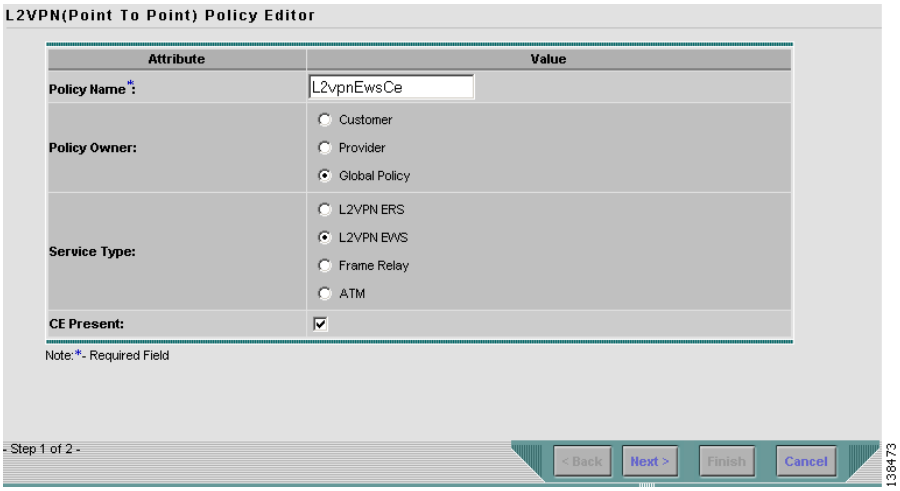
Step 23 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 24 Click **Finish**.

Defining an Ethernet EWS Policy with a CE

This section describes defining an Ethernet EWS policy with CE present. Figure 4-12 is an example of the first page of this policy.

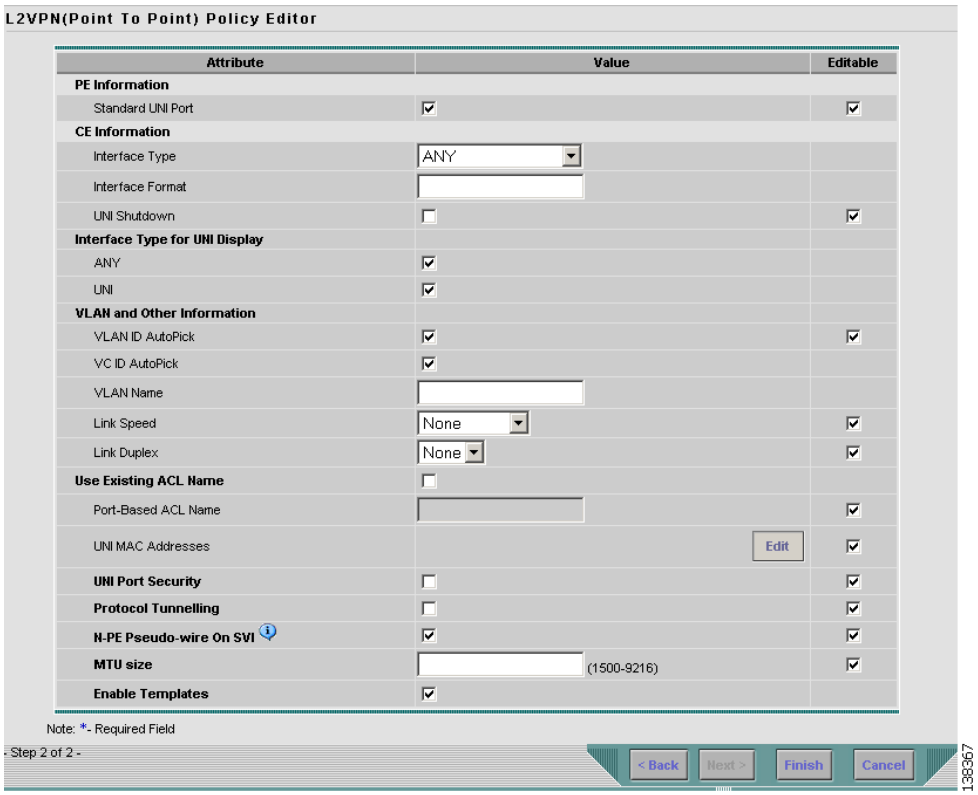
Figure 4-12 Ethernet EWS Policy with a CE



Step 1 Click **Next**. The window in Figure 4-13 appears.

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

Figure 4-13 Ethernet EWS with CE Policy Attributes



Step 2 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect 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.

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

You can choose to select 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**

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 policy.

Step 6 Select 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 Select 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 selected by default.

Step 8 Select 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 selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

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

Step 11 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. Two VLANs cannot share the same name.

Step 12 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

Step 13 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 14 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 15 Select the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this the check box is not selected 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 16 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 17 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect 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 18 Enter one or more Ethernet MAC addresses in **UNI MAC Addresses**.

Step 19 Select the **UNI Port Security** check box (see Figure 4-14) if you to 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.

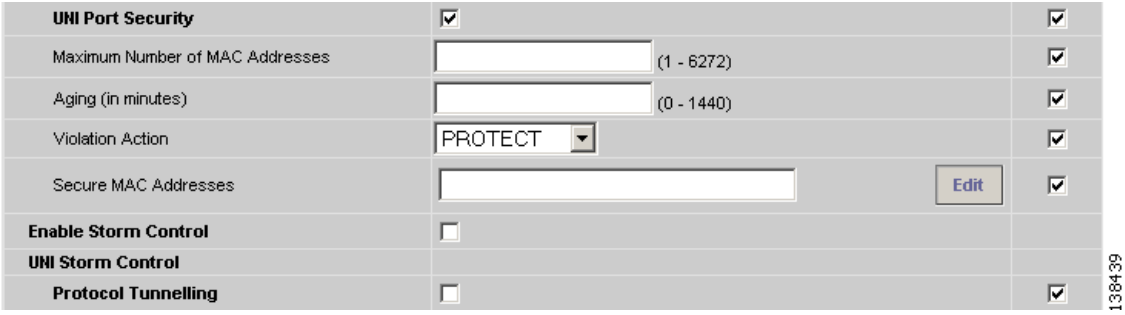
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

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.

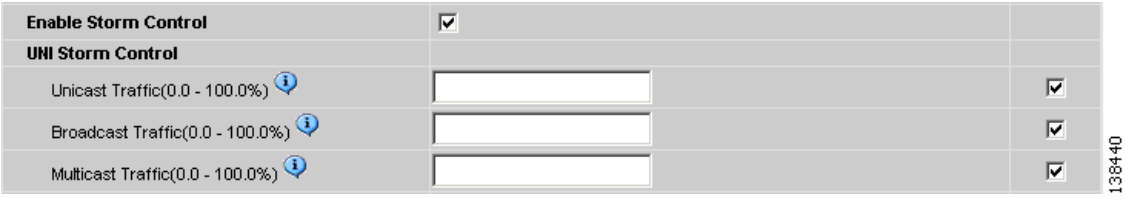
d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 4-14 UNI Port Security



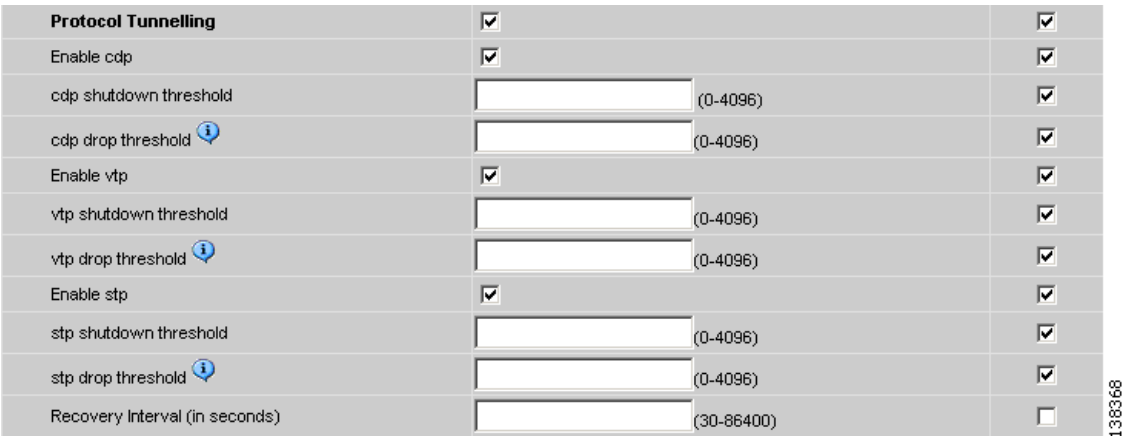
Step 20 Select the **Enable Storm Control** check box (see Figure 4-15) to help prevent the UNI port from being disrupted by a broadcast, multicast, or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage 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 4-15 Enable Storm Control



Step 21 Select the **Protocol Tunnelling** check box (see Figure 4-16) 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 4-16 Protocol Tunnelling



For each protocol that you select, 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 22 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If the check box is not selected, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 23 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 4.1, 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 4.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

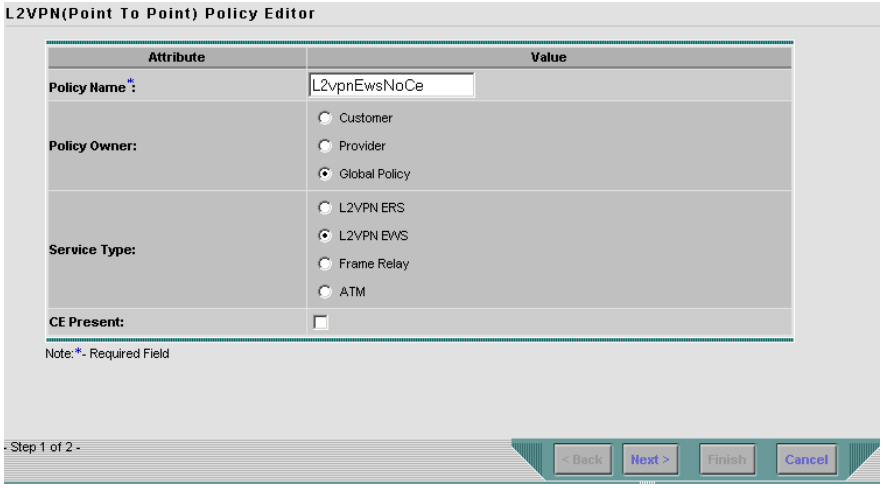
Step 24 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 25 Click **Finish**.

Defining an Ethernet EWS Policy without a CE

This section describes how to define an Ethernet EWS policy without a CE present. Figure 4-17 is an example of the first page of this policy.

Figure 4-17 Ethernet EWS Policy without a CE

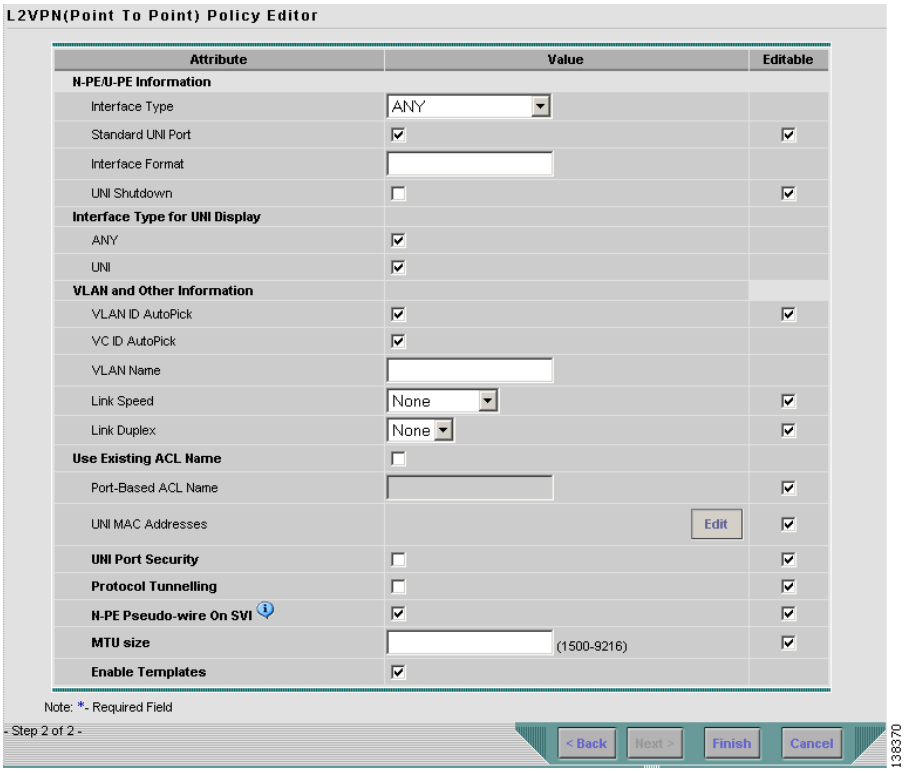


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-18 appears.

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

Figure 4-18 Ethernet EWS without CE Policy Attributes



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

You can choose to select 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**

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

Step 3 Select the **Standard UNI Port** check box to enable port security. This is the default. When you deselect 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.

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 policy.

Step 6 Select 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 Select 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 selected by default.

Step 8 Select 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 selected by default.

Step 9 Select the **VLANID AutoPick** check box if you want ISC to choose a VLAN ID. If you do not select this check box, you will be prompted to provide the VLAN in a Provider VLAN ID field during service activation.

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

Step 11 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. Two VLANs cannot share the same name.

Step 12 Enter a **Link Speed** (optional) of 10, 100, 1000, or auto.

Step 13 Enter a **Line Duplex** (optional) of full, half, or auto.

Step 14 Select 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 selected 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 15 Enter a **Port-Based ACL Name** (if you selected the **Use Existing ACL Name** check box, as mentioned in the previous step).

Step 16 Enter one or more Ethernet MAC addresses in **UNI MAC addresses**. This selection is present only if you deselect 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 17 Select the **UNI Port Security** check box (see Figure 4-6) if you to 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.

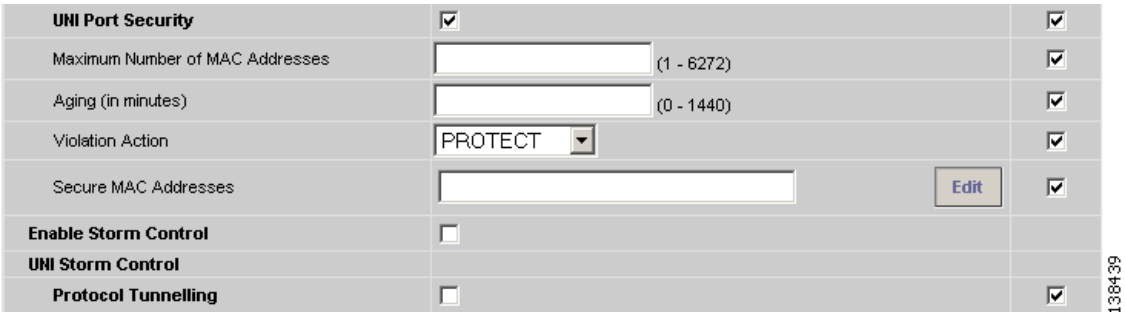
b. For **Aging,** enter the length of time the MAC address can stay on the port security table.

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.

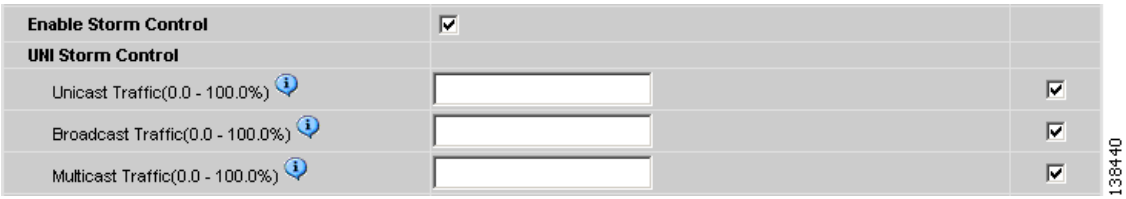
d. In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.

Figure 4-19 UNI Port Security



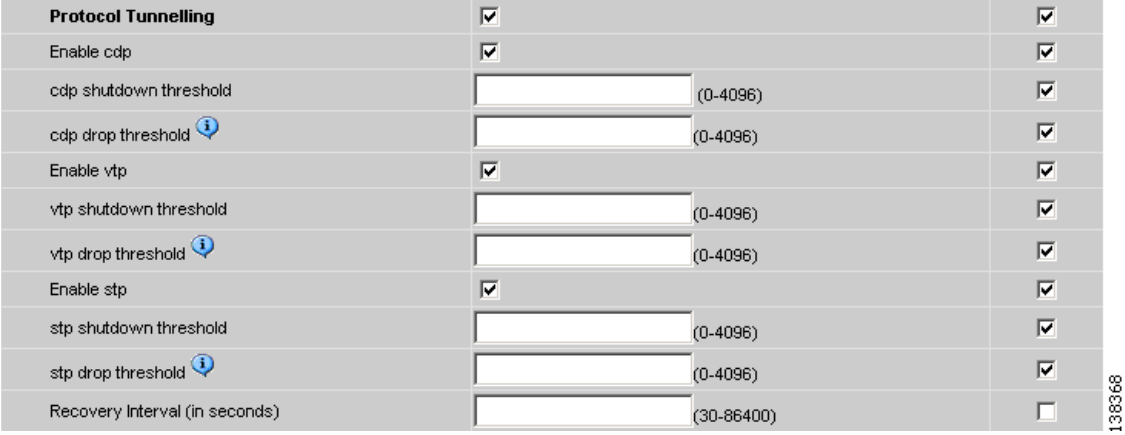
Step 18 Select the **Enable Storm Control** check box (see Figure 4-20) to help prevent the UNI port from being disrupted by a broadcast, multicast or unicast storm. Enter a threshold value for each type of traffic. The value, which can be specified to two significant digits, represents the percentage 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 4-20 Enable Storm Control



Step 19 Select the **Protocol Tunnelling** check box (see Figure 4-16) 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 4-21 Protocol Tunnelling



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 20 Select the **N-PE Psuedo-wire On SVI** check box to configure the pseudo-wire connection on the switched virtual interface of the OSM card. If the check box is not selected, the pseudo-wire will be provisioned on the sub-interface of the PFC card, if it is available. This option is only available for C76xx devices.

Step 21 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 4.1, 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 4.1 uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

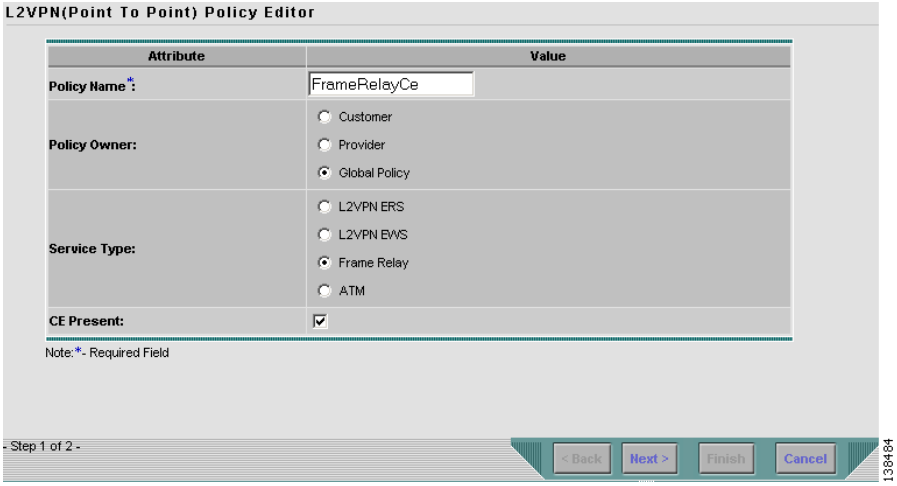
Step 22 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 23 Click **Finish**.

Defining a Frame Relay Policy with a CE

This section describes how to define a Frame Relay policy with CE present. Figure 4-22 is an example of the first page of this policy.

Figure 4-22 Frame Relay Policy with a CE

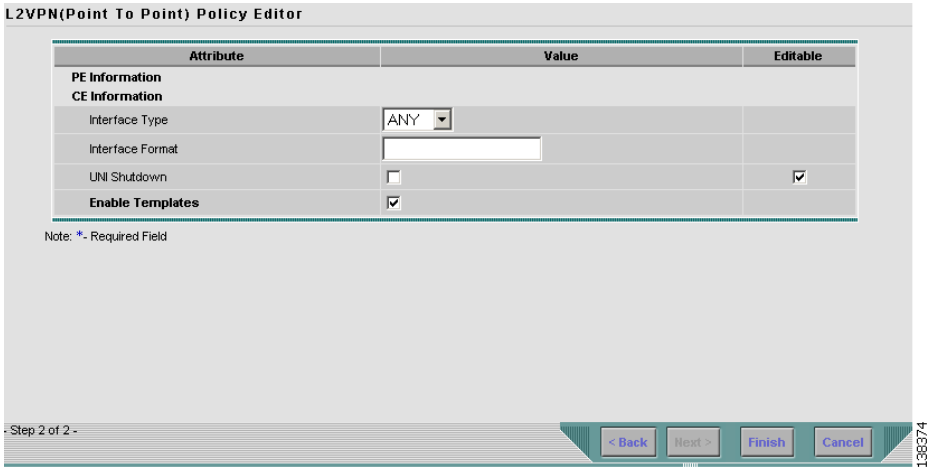


Perform the following steps:

Step 1 Click **Next**. The window in Figure 4-23 appears.

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

Figure 4-23 Frame Relay with CE Policy Attributes



Step 2 Choose the **Encapsulation** type for the PE from the drop-down list. The choices are:

- **FRAME RELAY**
- **FRAME RELAY IETF**

Step 3 Choose the **Interface Type** for the **CE** from the drop-down list. The choices are:

- **ANY**
- **Serial**
- **POS**
- **Hssi**
- **BRI**

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 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 6 Select 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.

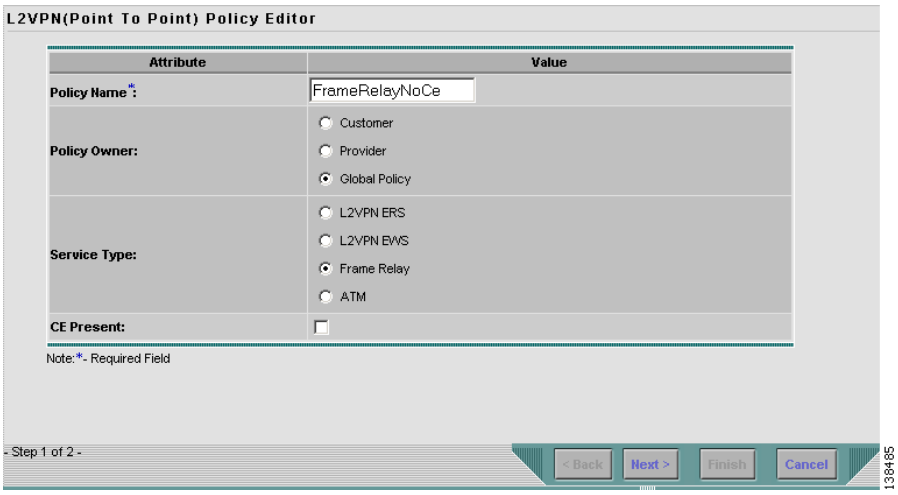
Step 7 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

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 4-24 is an example of the first page of this policy.

Figure 4-24 Frame Relay Policy without a CE

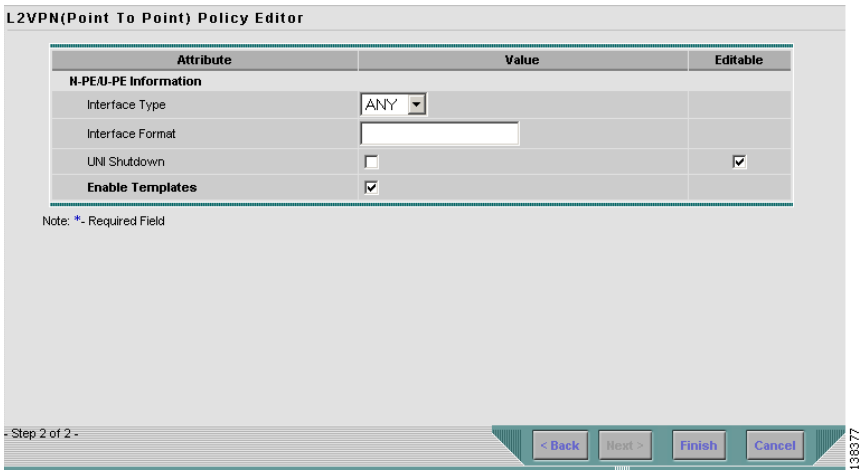


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-25 appears.

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

Figure 4-25 Frame Relay without CE Policy Attributes



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

- **ANY**
- **Serial**
- **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 Select 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.

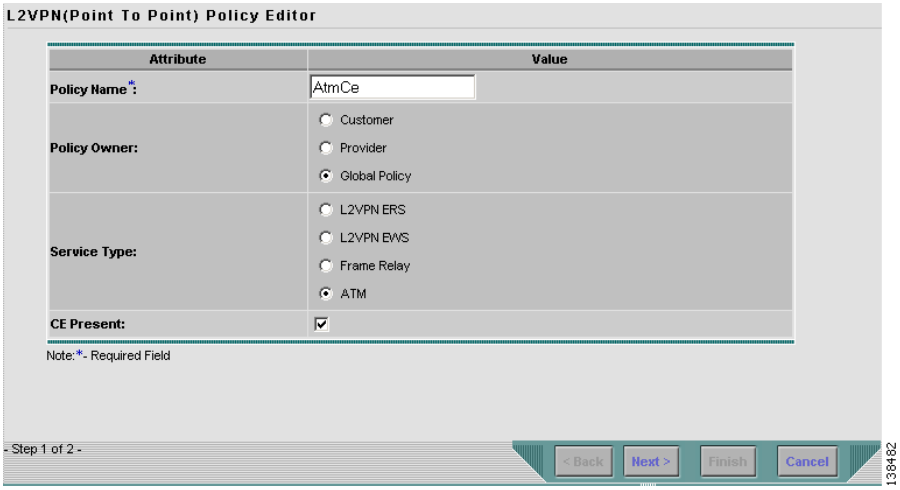
Step 6 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 7 Click **Finish**.

Defining an ATM Policy with a CE

This section describes how to define an AMT policy with CE present. Figure 4-26 is an example of the first page of this policy.

Figure 4-26 ATM Policy with a CE

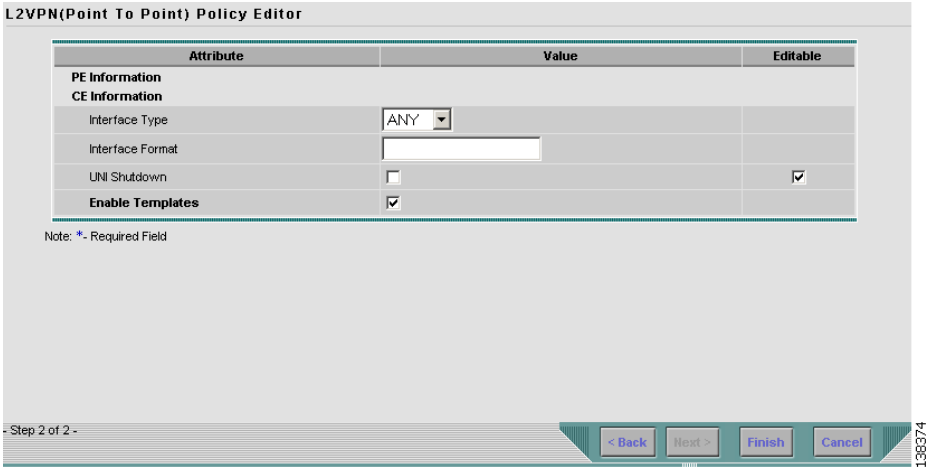


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-27 appears.

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

Figure 4-27 ATM with CE Policy Attributes



Step 2 Choose the **PE Encapsulation** type from the drop-down list. The choices are:

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

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 Select 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.

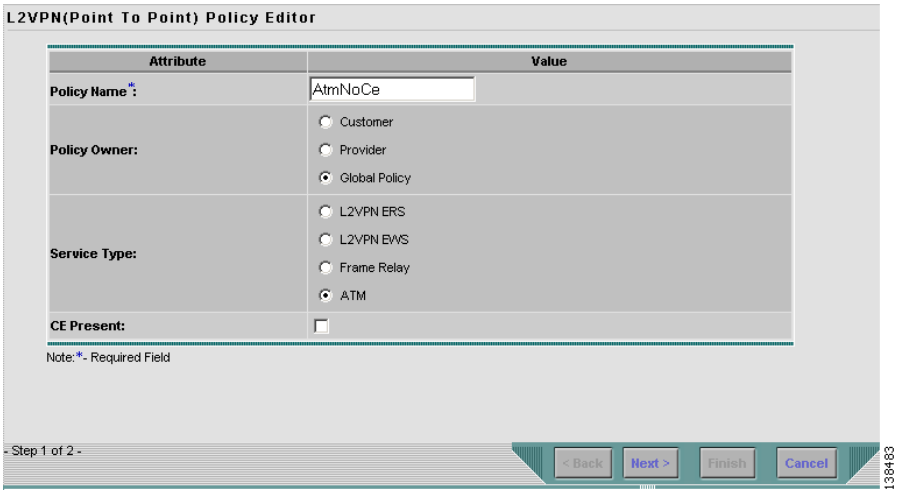
Step 7 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 8 Click **Finish**.

Defining an ATM Policy without a CE

This section describes how to define an AMT policy without a CE present. Figure 4-28 is an example of the first page of this policy.

Figure 4-28 ATM Policy without a CE

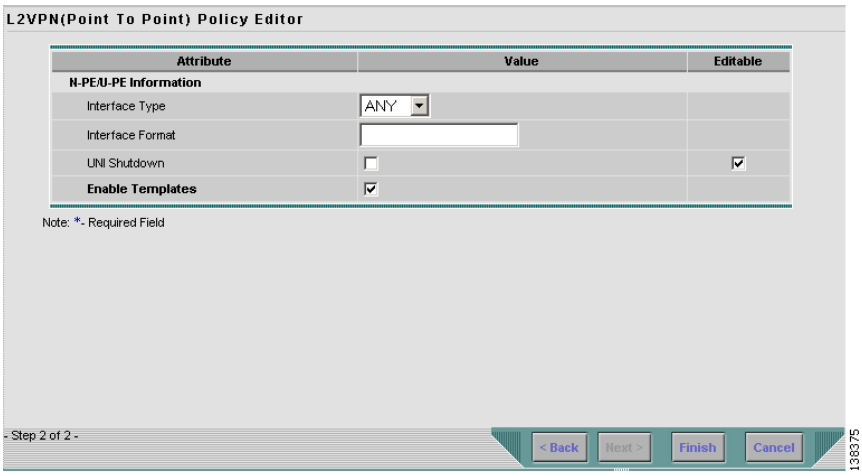


Perform the following steps.

Step 1 Click **Next**. The window in Figure 4-29 appears.

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

Figure 4-29 ATM without CE Policy Attributes



Step 2 Choose the **N-PE/U-PE Interface Type** from the drop-down list. The choices are:

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

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 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 5 Select 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 Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

Step 7 Click **Finish**.