



## CHAPTER 7

# Creating a VPLS Policy

---

This chapter contains the basic steps to create a VPLS policy. It contains the following sections:

- [Defining a VPLS Policy, page 7-1](#)
- [Defining an MPLS/ERMS \(EVP-LAN\) Policy with a CE, page 7-3](#)
- [Defining an MPLS/ERMS \(EVP-LAN\) Policy without a CE, page 7-7](#)
- [Defining an MPLS/EMS \(EP-LAN\) Policy with a CE, page 7-11](#)
- [Defining an MPLS/EMS \(EP-LAN\) Policy without a CE, page 7-16](#)
- [Defining an Ethernet/ERMS \(EVP-LAN\) Policy with a CE, page 7-23](#)
- [Defining an Ethernet/ERMS \(EVP-LAN\) Policy without a CE, page 7-27](#)
- [Defining an Ethernet/EMS \(EP-LAN\) Policy with a CE, page 7-32](#)
- [Defining an Ethernet/EMS \(EP-LAN\) Policy without a CE, page 7-38](#)

## Defining a VPLS Policy

You must define a VPLS policy before you can provision a service. A VPLS policy defines the common characteristics shared by the Attachment Circuit (AC) attributes.

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.

You can also associate Cisco IP Solution Center (ISC) templates and data files with a service request. See [Appendix B, “Working with Templates and Data Files,”](#) for more about using templates and data files in service requests.

VPLS policies correspond to the one of the core types that VPLS provides:

- MPLS core type—provider core network is MPLS enabled
- Ethernet core type—provider core network uses Ethernet switches

and to one of the service types that VPLS provides:

- Ethernet Relay Multipoint Service (ERMS). The Metro Ethernet Forum name for ERMS is Ethernet Virtual Private LAN (EVP-LAN). See [Layer 2 Terminology Conventions, page D-1](#) for more information about terms used to denote VPLS services in this guide.
- Ethernet Multipoint Service (EMS). The MEF name for EMS is Ethernet Private LAN (EP-LAN).

A policy is a template of most of the parameters needed to define a VPLS service request. After you define it, a VPLS policy can be used by all the VPLS service requests that share a common set of characteristics.

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

To define a VPLS policy in the Cisco IP Solution Center (ISC), perform the following steps.

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

The Policies window appears.

**Step 2** Click **Create**.

**Step 3** Choose **VPLS Policy**.

The VPLS Policy Editor window appears. (See [Figure 7-1](#).)

**Figure 7-1** Creating a VPLS Policy

The screenshot shows the VPLS Policy Editor window with the following fields and values:

Attribute	Value
Policy Name *	<input type="text"/>
Policy Owner:	<input checked="" type="radio"/> Customer <input type="radio"/> Provider <input type="radio"/> Global Policy
Customer *	<input type="text"/> <input type="button" value="Select"/>
Core Type *	<input checked="" type="radio"/> MPLS <input type="radio"/> Ethernet
Service Type *	<input checked="" type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input checked="" type="checkbox"/>

Note: \* - Required Field

Step 1 of 3 -

**Step 4** Enter a **Policy Name** for the VPLS policy.

**Step 5** Choose the **Policy Owner** for the VPLS policy.

There are three types of VPLS policy ownership:

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

This ownership has relevance when the ISC Role-Based Access Control (RBAC) comes into play. For example, a VPLS 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 6** Click **Select** to choose the owner of the VPLS policy.

The policy owner was established when you created customers or providers during ISC setup. If the ownership is global, the Select function does not appear.

**Step 7** Choose the **Core Type** of the VPLS policy.

There are two core types for VPLS policies:

- MPLS—running on an IP network
- Ethernet—all PEs are on an Ethernet provider network

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

There are two service types for VPLS policies:

- Ethernet Relay Multipoint Service (ERMS). (The MEF name for ERMS is EVP-LAN.)
- Ethernet Multipoint Service (EMS). (The MEF name for EMS is EP-LAN.)

**Step 9** Check the **CE Present** check box if you want ISC to ask the service operator who uses this VPLS 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 PE router and customer-facing interface.

## Defining an MPLS/ERMS (EVP-LAN) Policy with a CE

This section describes how to define a VPLS policy with an MPLS core type and an ERMS (EVP-LAN) service type with CE present. [Figure 7-2](#) is an example of the first page of this policy.

**Figure 7-2** MPLS/ERMS (EVP-LAN) Policy with a CE

The screenshot shows the 'VPLS Policy Editor' window. It contains a table with 'Attribute' and 'Value' columns. The 'Policy Name' is 'VplsMplsErmsCe'. The 'Policy Owner' has radio buttons for 'Customer', 'Provider', and 'Global Policy' (selected). The 'Core Type' has radio buttons for 'MPLS' (selected) and 'Ethernet'. The 'Service Type' has radio buttons for 'Ethernet Relay Multipoint Service (ERMS)' (selected) and 'Ethernet Multipoint Service (EMS)'. The 'CE Present' checkbox is checked. A note at the bottom left says 'Note: \*- Required Field'. At the bottom right, there are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'. The status bar at the bottom left says '- Step 1 of 3 -' and the bottom right has the number '204781'.

Attribute	Value
Policy Name *	VplsMplsErmsCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input checked="" type="radio"/> MPLS <input type="radio"/> Ethernet
Service Type *	<input checked="" type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input checked="" type="checkbox"/>

Note: \*- Required Field

- Step 1 of 3 -

< Back Next > Finish Cancel

204781

Perform the following steps.

**Step 1** Click **Next**. The window in [Figure 7-3](#) 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 VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 7-3 MPLS/ERMS (EVP-LAN) with a CE Policy Attributes

VPLS Policy Editor

Attribute	Value	Editable
<b>CE Information</b>		
Interface Type	ANY	
Interface Format		
<b>UNI Information</b>		
Standard UNI Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses		<input checked="" type="checkbox"/>
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PE/UNI Interface Description:		<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name		
<b>Use Existing ACL Name</b>		
Port-Based ACL Name		<input checked="" type="checkbox"/>
Disable CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Filter BPDU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \* Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211696

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

You can choose a particular interface on a CE, N-PE, PE-AGG, 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

**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 a CE **Encapsulation** type.

The choices are:

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

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

**Step 5** 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.

**Step 6** Check **UNI Shutdown** 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** 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 11** Choose a **Port Type**.

The choices are:

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

**Step 12** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

**Step 13** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

**Step 14** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.

**Step 15** 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 16** 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 17** 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

**Step 20** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

**Step 21** Check the **UNI Port Security** check box (see [Figure 7-4](#)) 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. Click the **Edit** button to enter the addresses.

**Figure 7-4** UNI Port Security

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

204776

**Step 22** Check the **Enable Storm Control** check box (see [Figure 7-5](#)) 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 7-5 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"/>

**Step 23** 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 24** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

## Defining an MPLS/ERMS (EVP-LAN) Policy without a CE

This section describes defining a VPLS policy with an MPLS core type and an ERMS (EVP-LAN) service type without a CE present. [Figure 7-6](#) is an example of the first page of this policy.

Figure 7-6 MPLS/ERMS (EVP-LAN) Policy without a CE

VPLS Policy Editor

Attribute	Value
Policy Name *	VplsMplsErmsNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input checked="" type="radio"/> MPLS <input type="radio"/> Ethernet
Service Type *	<input checked="" type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input type="checkbox"/>

Note: \*- Required Field

- Step 1 of 3 -

< Back Next > Finish Cancel

Perform the following steps.

**Step 1** Click **Next**. The window in [Figure 7-7](#) 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 VPLS policy can modify the editable parameter during VPLS service request creation.

**Figure 7-7** MPLS/ERMS (EVP-LAN) without a CE Policy Attributes

VPLS Policy Editor

Attribute	Value	Editable
<b>N-PE/U-PE Information</b>		
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"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses	<input type="text"/>	<input checked="" type="checkbox"/> Edit
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PE/UNI Interface Description:	<input type="text"/>	<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name	<input type="text"/>	
<b>Use Existing ACL Name</b>		
Port-Based ACL Name	<input type="text"/>	<input checked="" type="checkbox"/>
Disable CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Filter BPDU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \*. Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211697

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

You can choose a particular interface on a N-PE, U-PE, or PE-AGG 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

- 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.
- 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** type.
- The choices are:
- **DOT1Q**
  - **DEFAULT**
- If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.
- Step 6** Check **UNI Shutdown** 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** 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 11** Choose a **Port Type**.
- The choices are:
- **Access Port**
  - **Trunk with Native VLAN**
- Step 12** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 13** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 14** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.
- Step 15** 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 16** 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 17** 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

**Step 20** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

**Step 21** Check the **UNI Port Security** check box (see [Figure 7-8](#)) 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 7-8** UNI Port Security




<b>UNI Port Security</b>	<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="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

**Step 22** Check the **Enable Storm Control** check box (see [Figure 7-9](#)) 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 7-9 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 23** 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 24** Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

## Defining an MPLS/EMS (EP-LAN) Policy with a CE

This section describes defining a VPLS policy with an MPLS core type and an EMS (EP-LAN) service type with CE present. [Figure 7-10](#) is an example of the first page of this policy.

Figure 7-10 MPLS/EMS (EP-LAN) Policy with a CE

VPLS Policy Editor

Attribute	Value
Policy Name *	VplsMplsEmsCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input checked="" type="radio"/> MPLS <input type="radio"/> Ethernet
Service Type *	<input type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input checked="" type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input checked="" type="checkbox"/>

Note: \*- Required Field

- Step 1 of 3 -

204783

Perform the following steps.

**Step 1** Click **Next**. The window in [Figure 7-11](#) 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 VPLS policy can modify the editable parameter during VPLS service request creation.

**Figure 7-11** MPLS/EMS (EP-LAN) with a CE Policy Attributes

Attribute	Value	Editable
<b>CE Information</b>		
Interface Type	ANY	
Interface Format		
<b>UNI Information</b>		
Standard UNI Port	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses	<input type="text"/>	<input checked="" type="checkbox"/>
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PE/UNI Interface Description:	<input type="text"/>	<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name	<input type="text"/>	
System MTU (in bytes)	1522 (1500-9216)	<input checked="" type="checkbox"/>
<b>Use Existing ACL Name</b>		
Port-Based ACL Name	<input type="text"/>	<input checked="" type="checkbox"/>
Disable CDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Protocol Tunneling</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \* - Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

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

You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

- 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 a CE **Encapsulation** type.

The choices are:

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



**Note**

When creating a service request based on the MPLS/EMS (EP-LAN) with CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.

- Step 5** 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.

- 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** 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 10** 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 11** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

- Step 12** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

- Step 13** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.

- Step 14** 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 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. Two VLANs cannot share the same name.
- Step 16** Enter the **System MTU** in bytes.  
The maximum transmission unit (MTU) size is configurable and optional. 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. ISC supports, ranges for different platforms, as specified below. The range is 1500 to 9216.
- 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 uses 9216 in both cases.
  - For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.
- Step 17** 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.
- Step 20** Check the **UNI Port Security** check box (see [Figure 7-12](#)) 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 7-12 UNI Port Security**

<b>UNI Port Security</b>	<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="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

- Step 21** Check the **Enable Storm Control** check box (see [Figure 7-13](#)) 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 7-13 Enable Storm Control**

<b>Enable Storm Control</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Storm Control</b>		
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 22** Check the **Protocol Tunnelling** check box (see [Figure 7-14](#)) 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 7-14 Protocol Tunnelling**

<b>Protocol Tunnelling</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CDP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
cdp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Tunnel VTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VTP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
vtp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Tunnel STP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
STP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
stp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Recovery Interval (in seconds)	<input type="text"/> (30-86400)	<input checked="" type="checkbox"/>

138441

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

- a. **Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- b. **CDP 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. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **VTP 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. **Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **STP 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 23** 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 24** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

## Defining an MPLS/EMS (EP-LAN) Policy without a CE

This section describes defining a VPLS policy with an MPLS core type and an EMS (EP-LAN) service type without a CE present. [Figure 7-15](#) is an example of the first page of this policy.

**Figure 7-15** MPLS/EMS (EP-LAN) Policy without a CE

The screenshot shows the 'VPLS Policy Editor' window. It contains a table with two columns: 'Attribute' and 'Value'. The table has the following rows:

Attribute	Value
Policy Name *	VplsMplsEmsNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input checked="" type="radio"/> MPLS <input type="radio"/> Ethernet
Service Type *	<input type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input checked="" type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input type="checkbox"/>

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 3 -' and the bottom right has the number '204784'.

Perform the following steps.

- Step 1** Click **Next**. The window in [Figure 7-16](#) appears.

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

Figure 7-16 MPLS/EMS (EP-LAN) without a CE Policy Attributes

VPLS Policy Editor

Attribute	Value	Editable
<b>N-PE/U-PE Information</b>		
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"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses		<input checked="" type="checkbox"/> <input type="button" value="Edit"/>
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PE/UNI Interface Description:		<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name		
System MTU (in bytes)		<input checked="" type="checkbox"/> (1500-9216)
<b>Use Existing ACL Name</b>		
Port-Based ACL Name		<input checked="" type="checkbox"/>
Disable CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>		
Protocol Tunneling	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \*- Required Field

- Step 2 of 3 -

211699

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


You can choose a particular interface on a N-PE, U-PE, or PE-AGG 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

**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.

- 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 N-PE/U-PE **Encapsulation** type.
- The choices are:
- **DOT1Q**
  - **DEFAULT**
-  **Note** When creating a service request based on the MPLS/EMS (EP-LAN) without CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.
- 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** 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 11** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 12** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 13** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.
- Step 14** 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 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. Two VLANs cannot share the same name.
- Step 16** Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. 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. ISC supports, ranges for different platforms, as specified below. The range is 1500 to 9216.

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

**Step 17** 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

**Step 20** Check the **UNI Port Security** check box (see [Figure 7-17](#)) 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 7-17 UNI Port Security**

<b>UNI Port Security</b>	<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="button" value="Edit"/>	<input checked="" type="checkbox"/>

- Step 21** Check the **Enable Storm Control** check box (see [Figure 7-18](#)) 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 7-18 Enable Storm Control**

<b>Enable Storm Control</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Storm Control</b>		
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"/>

- Step 22** Check the **Protocol Tunnelling** check box (see [Figure 7-19](#)) 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 7-19 Protocol Tunnelling**

<b>Protocol Tunnelling</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CDP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
cdp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Tunnel VTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VTP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
vtp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Tunnel STP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
STP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
stp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Recovery Interval (in seconds)	<input type="text"/> (30-86400)	<input checked="" type="checkbox"/>

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

- Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- CDP 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. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **VTP 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. **Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **STP 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 23** 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 24** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

## Defining an Ethernet/ERMS (EVP-LAN) Policy with a CE

This section describes defining a VPLS policy with an Ethernet core type and an ERMS (EVP-LAN) service type with CE present. [Figure 7-20](#) is an example of the first page of this policy.

**Figure 7-20** Ethernet/ERMS (EVP-LAN) Policy with a CE

The screenshot shows the 'VPLS Policy Editor' window. It contains a table with two columns: 'Attribute' and 'Value'. The table has the following rows:

Attribute	Value
Policy Name *	VplsEtherErmsCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input type="radio"/> MPLS <input checked="" type="radio"/> Ethernet
Service Type *	<input checked="" type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input checked="" type="checkbox"/>

Below the table, there is a note: 'Note: \*- Required Field'. At the bottom of the window, there is a progress indicator '- Step 1 of 3 -' and four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. A small number '204785' is visible in the bottom right corner of the window.

Perform the following steps.

### Step 1 Click Next.

The window in [Figure 7-21](#) 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 VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 7-21 Ethernet ERMS (EVP-LAN) with a CE Policy Attributes

VPLS Policy Editor

Attribute	Value	Editable
<b>CE Information</b>		
Interface Type	ANY	
Interface Format		
<b>UNI Information</b>		
Standard UNI Port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses		<input checked="" type="checkbox"/>
		<input type="button" value="Edit"/>
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PE/UNI Interface Description:		<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name		
<b>Use Existing ACL Name</b>		
Port-Based ACL Name		<input checked="" type="checkbox"/>
Disable CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Filter BPDU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \*- Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211700

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

You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

**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 a CE **Encapsulation** type.
- The choices are:
- **DOT1Q**
  - **DEFAULT**
- If **DEFAULT** is the CE encapsulation type, ISC shows another field for the UNI port type.
- Step 5** 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.
- 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** 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 11** Choose a **Port Type**.
- The choices are:
- **Access Port**
  - **Trunk with Native VLAN**
- Step 12** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 13** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 14** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.
- Step 15** 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 16** 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 17** 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

**Step 20** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

**Step 21** Check the **UNI Port Security** check box (see [Figure 7-22](#)) 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 7-22 UNI Port Security**




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

204776

**Step 22** Check the **Enable Storm Control** check box (see [Figure 7-22](#)) 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 7-23 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 23** 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 24** Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

## Defining an Ethernet/ERMS (EVP-LAN) Policy without a CE

This section describes defining a VPLS policy with an Ethernet core type and an ERMS (EVP-LAN) service type without a CE present. [Figure 7-24](#) is an example of the first page of this policy.

Figure 7-24 Ethernet/ERMS (EVP-LAN) Policy without a CE

VPLS Policy Editor

Attribute	Value
Policy Name *	VplsEtherErmsNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input type="radio"/> MPLS <input checked="" type="radio"/> Ethernet
Service Type *	<input checked="" type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input type="checkbox"/>

Note: \*- Required Field

- Step 1 of 3 -

< Back Next > Finish Cancel

204786

Perform the following steps.

**Step 1** Click **Next**.

The window in [Figure 7-25](#) 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 VPLS policy can modify the editable parameter during VPLS service request creation.

**Figure 7-25** Ethernet/ERMS (EVP-LAN) without a CE Policy Attributes

The screenshot shows the VPLS Policy Editor window with the following attributes and values:

Attribute	Value	Editable
<b>N-PEU-PE Information</b>		
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"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses		<input checked="" type="checkbox"/>
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PE/UNI Interface Description:		<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name		
<b>Use Existing ACL Name</b>		
Port-Based ACL Name		<input checked="" type="checkbox"/>
Disable CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Filter BPDU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \* - Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

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

You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

**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.

**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** type.

The choices are:

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

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

**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** 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 11** Choose a **Port Type**.

The choices are:

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

**Step 12** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

**Step 13** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

**Step 14** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.

**Step 15** 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 16** 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 17** 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.
- Step 20** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).
- Step 21** Check the **UNI Port Security** check box (see [Figure 7-26](#)) 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.
- 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 7-26** UNI Port Security




<b>UNI Port Security</b>	<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 checked="" type="checkbox"/>

204776

- Step 22** Check the **Enable Storm Control** check box (see [Figure 7-27](#)) 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 7-27 Enable Storm Control**

<b>Enable Storm Control</b>	<input checked="" type="checkbox"/>	
<b>UNI Storm Control</b>		
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 23** 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 24** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

## Defining an Ethernet/EMS (EP-LAN) Policy with a CE

This section describes defining a VPLS policy with an Ethernet core type and an EMS (EP-LAN) service type with a CE present. [Figure 7-28](#) is an example of the first page of this policy.

**Figure 7-28** Ethernet/EMS (EP-LAN) Policy with CE Present

The screenshot shows the 'VPLS Policy Editor' window. It contains a table with two columns: 'Attribute' and 'Value'. The attributes and their values are as follows:

Attribute	Value
Policy Name *	VplsEtherEmsCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input type="radio"/> MPLS <input checked="" type="radio"/> Ethernet
Service Type *	<input type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input checked="" type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input checked="" type="checkbox"/>

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 3 -".

Perform the following steps.

### Step 1 Click Next.

The window in [Figure 7-29](#) 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 VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 7-29 Ethernet/EMS (EP-LAN) with a CE Policy Attributes

VPLS Policy Editor

Attribute	Value	Editable
<b>CE Information</b>		
Interface Type	ANY	
Interface Format		
<b>UNI Information</b>		
Standard UNI Port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UNI Shutdown	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Keep Alive	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses		<input checked="" type="checkbox"/>
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PEUNI Interface Description:		<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name		
System MTU (in bytes)	1522 (1500-9216)	<input checked="" type="checkbox"/>
<b>Use Existing ACL Name</b>		
Port-Based ACL Name		<input checked="" type="checkbox"/>
Disable CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Protocol Tunneling</b>		
	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \* Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211702

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

You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

**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 a CE **Encapsulation** type.

The choices are:

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



**Note**

---

When creating a service request based on the Ethernet/EMS (EP-LAN) with CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.

---

**Step 5** 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.

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

**Step 12** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

**Step 13** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.

**Step 14** 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 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. Two VLANs cannot share the same name.

**Step 16** Enter the **System MTU** 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 17** Check the **Use Existing ACL Name** check box if you want assign your own named access list to the port. By default, this 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

**Step 20** Check the **UNI Port Security** check box (see [Figure 7-30](#)) 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 7-30 UNI Port Security

<b>UNI Port Security</b>	<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="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

- Step 21** Check the **Enable Storm Control** check box (see Figure 7-31) 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 7-31 Enable Storm Control

<b>Enable Storm Control</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Storm Control</b>		
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 22** Check the **Protocol Tunnelling** check box (see Figure 7-32) 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 7-32 Protocol Tunnelling

<b>Protocol Tunnelling</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CDP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
cdp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Tunnel VTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VTP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
vtp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Tunnel STP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
STP Threshold (in packets/seconds)	<input type="text"/> (0-4096)	<input checked="" type="checkbox"/>
stp drop threshold	<input type="text"/> (0-4096)	<input type="checkbox"/>
Recovery Interval (in seconds)	<input type="text"/> (30-86400)	<input checked="" type="checkbox"/>

138441

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

- Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- CDP 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. **Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- e. **VTP 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. **Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).
- h. **STP 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 23** 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 24** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

## Defining an Ethernet/EMS (EP-LAN) Policy without a CE

This section describes defining a VPLS policy with an Ethernet core type and an EMS (EP-LAN) service type without a CE present. [Figure 7-33](#) is an example of the first page of this policy.

**Figure 7-33** Ethernet/EMS (EP-LAN) Policy without a CE

The screenshot shows the VPLS Policy Editor window with the following configuration:

Attribute	Value
Policy Name *	VplsEtherEmsNoCe
Policy Owner:	<input type="radio"/> Customer <input type="radio"/> Provider <input checked="" type="radio"/> Global Policy
Core Type *	<input type="radio"/> MPLS <input checked="" type="radio"/> Ethernet
Service Type *	<input type="radio"/> Ethernet Relay Multipoint Service (ERMS) <input checked="" type="radio"/> Ethernet Multipoint Service (EMS)
CE Present:	<input type="checkbox"/>

Note: \* - Required Field

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

Page number: 204788

Perform the following steps.

### Step 1 Click Next.

The window in [Figure 7-34](#) 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 VPLS policy can modify the editable parameter during VPLS service request creation.

Figure 7-34 Ethernet/EMS (EP-LAN) without CE Policy Attributes

VPLS Policy Editor

Attribute	Value	Editable
<b>N-PEU-PE Information</b>		
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"/>
<b>Interface Type for UNI Display</b>		
ANY	<input checked="" type="checkbox"/>	
UNI	<input checked="" type="checkbox"/>	
UNI MAC Addresses		<input checked="" type="checkbox"/>
Link Speed	None	<input checked="" type="checkbox"/>
Link Duplex	None	<input checked="" type="checkbox"/>
<b>VLAN and Other Information</b>		
PE/UNI Interface Description:		<input checked="" type="checkbox"/>
VLAN ID AutoPick	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN Name		
System MTU (in bytes)	(1500-9216)	<input checked="" type="checkbox"/>
<b>Use Existing ACL Name</b>		
Port-Based ACL Name		<input checked="" type="checkbox"/>
Disable CDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>UNI Port Security</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Protocol Tunneling</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Note: \*- Required Field

- Step 2 of 3 -

< Back Next > Finish Cancel

211703

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

You can choose a particular interface on a CE, N-PE, U-PE, or PE-AGG 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 VPLS service request creation. If defined as ANY, the operator can see all interface types.

**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.

**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 N-PE/U-PE **Encapsulation** type.

The choices are:

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



**Note**

When creating a service request based on the Ethernet/EMS (EP-LAN) without CE policy, the Encapsulation attribute is ignored. Therefore, setting this value has no effect.

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

**Step 12** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

**Step 13** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.

**Step 14** 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 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. Two VLANs cannot share the same name.

**Step 16** Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. 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. ISC supports, ranges for different platforms, as specified below. The range is 1500 to 9216.

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

**Step 17** 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 18** 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 19** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

**Step 20** Check the **UNI Port Security** check box (see [Figure 7-35](#)) 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.

- 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 7-35** UNI Port Security




<b>UNI Port Security</b>	<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="button" value="Edit"/>	<input checked="" type="checkbox"/>

204776

- Step 21** Check the **Enable Storm Control** check box (see [Figure 7-36](#)) 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 7-36 Enable Storm Control**

<b>Enable Storm Control</b>	<input checked="" type="checkbox"/>	
<b>UNI Storm Control</b>		
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 22** Check the **Protocol Tunnelling** check box (see [Figure 7-37](#)) 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 7-37 Protocol Tunnelling**

<b>Protocol Tunnelling</b>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Tunnel CDP	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
CDP Threshold (in packets/seconds)	<input type="text"/>	(0-4096)	<input checked="" type="checkbox"/>
cdp drop threshold	<input type="text"/>	(0-4096)	<input type="checkbox"/>
Tunnel VTP	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
VTP Threshold (in packets/seconds)	<input type="text"/>	(0-4096)	<input checked="" type="checkbox"/>
vtp drop threshold	<input type="text"/>	(0-4096)	<input type="checkbox"/>
Tunnel STP	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
STP Threshold (in packets/seconds)	<input type="text"/>	(0-4096)	<input checked="" type="checkbox"/>
stp drop threshold	<input type="text"/>	(0-4096)	<input type="checkbox"/>
Recovery Interval (in seconds)	<input type="text"/>	(30-86400)	<input checked="" type="checkbox"/>

138441

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

- Tunnel CDP**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).
- CDP 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.
- Tunnel VTP**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).
- VTP 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.
- Tunnel STP**—Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

- h. **STP 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 23** 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 24** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, ISC will “auto pick” this value. However, you can set this manually, if desired. This is done by editing the associated VPN configuration. The Edit VPN window has an **Enable VPLS** check box. When you check this box, you can manually enter a VPN ID in a field provided. For more information on creating and modifying VPNs, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

