



# CHAPTER 14

## 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 14-1](#)
- [Defining an MPLS/ERMS \(EVP-LAN\) Policy with a CE, page 14-3](#)
- [Defining an MPLS/ERMS \(EVP-LAN\) Policy without a CE, page 14-6](#)
- [Defining an MPLS/EMS \(EP-LAN\) Policy with a CE, page 14-8](#)
- [Defining an MPLS/EMS \(EP-LAN\) Policy without a CE, page 14-12](#)
- [Defining an Ethernet/ERMS \(EVP-LAN\) Policy with a CE, page 14-15](#)
- [Defining an Ethernet/ERMS \(EVP-LAN\) Policy without a CE, page 14-18](#)
- [Defining an Ethernet/EMS \(EP-LAN\) Policy with a CE, page 14-21](#)
- [Defining an Ethernet/EMS \(EP-LAN\) Policy without a CE, page 14-25](#)

## 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 Prime Fulfillment templates and data files with a service request. See [Chapter 49, “Using Templates and Data Files with Policies and Service Requests,”](#) 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). For more information about terms used to denote VPLS services in this guide, see the section “Layer 2 Terminology Conventions” in the L2VPN Concepts chapter in the [Cisco Prime Fulfillment Theory of Operations Guide 6.1](#).

- 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 Prime Fulfillment, perform the following steps.

---

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

The Policy Manager window appears.

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

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

The Create New VPLS Policy window appears.

**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 Prime Fulfillment 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 Prime Fulfillment 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 Prime Fulfillment 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, Prime Fulfillment 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.

Perform the following steps.

- 
- Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.
- Step 2** For Core Type, choose **MPLS**.
- Step 3** For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.
- Step 4** Check the **CE Present** check box.
- Step 5** Click **Next**.
- The Interface Type window appears.
- Step 6** 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 7** 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 8** Choose a CE **Encapsulation** type.
- The choices are:
- **DOT1Q**
  - **DEFAULT**
- If **DEFAULT** is the CE encapsulation type, Prime Fulfillment shows another field for the UNI port type.
- Step 9** 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 10** 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 11** 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 12** 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 13** 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 14** 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 15** Choose a **Port Type**.
- The choices are:
- **Access Port**
  - **Trunk with Native VLAN**
- Step 16** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 17** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 18** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.
- Step 19** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 20** 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 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).
- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).

**Note**

Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.
- Step 24** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).
- Step 25** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
  - For **Aging**, enter the length of time the MAC address can stay on the port security table.
  - For **Violation Action**, choose what action will occur when a port security violation is detected:
    - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
    - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
    - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
  - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses. Click the **Edit** button to enter the addresses.
- Step 26** Check the **Enable Storm Control** check box 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.
- Step 27** Click the **Next** button, if you want to enable template support for the policy.
- The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Chapter 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.
- Step 28** Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)

## 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.

Perform the following steps.

- 
- Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.
- Step 2** For Core Type, choose **MPLS**.
- Step 3** For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.
- Step 4** Uncheck the **CE Present** check box.
- Step 5** Click **Next**.  
The Interface Type window appears.
- Step 6** 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 7** 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 8** 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 9** Choose a CE **Encapsulation** type.  
The choices are:
- **DOT1Q**
  - **DEFAULT**
- If **DEFAULT** is the CE encapsulation type, Prime Fulfillment shows another field for the UNI port type.
- Step 10** 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 11** 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 12** 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 13** 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 14** 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 15** Choose a **Port Type**.
- The choices are:
- **Access Port**
  - **Trunk with Native VLAN**
- Step 16** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 17** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 18** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.
- Step 19** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 20** 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 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).
- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



**Note** Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.
- Step 24** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

- Step 25** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
  - For **Aging**, enter the length of time the MAC address can stay on the port security table.
  - For **Violation Action**, choose what action will occur when a port security violation is detected:
    - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
    - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
    - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
  - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.
- Step 26** Check the **Enable Storm Control** check box 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.
- Step 27** Click the **Next** button, if you want to enable template support for the policy.
- The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Appendix 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.
- Step 28** Click **Finish**.

**Note**


The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)

## 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.

Perform the following steps.



- 
- Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.
- Step 2** For Core Type, choose **MPLS**.
- Step 3** For Service Type, choose **Ethernet Multipoint Service (EMS)**.
- Step 4** Check the **CE Present** check box.
- Step 5** Click **Next**.  
The Interface Type window appears.
- Step 6** 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 7** 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 8** 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 9** 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 10** 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 11** 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 12** 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 13** 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 14** 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 15** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

**Step 16** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

**Step 17** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.

**Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 19** 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 20** Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. Prime Fulfillment 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. Prime Fulfillment 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, Prime Fulfillment uses 9216 in both cases.
- For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.

**Step 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

**Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



**Note** Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.
- Step 24** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.
- For **Maximum Number of MAC address**, enter the number of MAC addresses allowed for port security.
  - For **Aging**, enter the length of time the MAC address can stay on the port security table.
  - For **Violation Action**, choose what action will occur when a port security violation is detected:
    - PROTECT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value.
    - RESTRICT**—Drops packets with unknown source addresses until a sufficient number of secure MAC addresses are removed to drop below the maximum value and causes the Security Violation counter to increment.
    - SHUTDOWN**—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.
  - In the **Secure MAC Addresses** field, enter one or more Ethernet MAC addresses.
- Step 25** Check the **Enable Storm Control** check box 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.
- Step 26** Check the **Protocol Tunnelling** check box 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.
- 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).
  - STP Threshold**—Enter the number of packets per second to be received before the interface is shut down.
  - stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.
  - Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.
- Step 27** Click the **Next** button, if you want to enable template support for the policy.

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Chapter 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Step 28** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)

## 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.

Perform the following steps.

**Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.

**Step 2** For Core Type, choose **MPLS**.

**Step 3** For Service Type, choose **Ethernet Multipoint Service (EMS)**.

**Step 4** Uncheck the **CE Present** check box.

**Step 5** Click **Next**.


The Interface Type window appears.

**Step 6** 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 7** 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 8** 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 9** 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 10** 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 11** 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 12** 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 13** 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 14** 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 15** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 16** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 17** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.
- Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 19** 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 20** Enter the **System MTU** in bytes.

The maximum transmission unit (MTU) size is configurable and optional. Prime Fulfillment 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.

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

- Step 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).
- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



**Note** Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.
- Step 24** Check the **UNI Port Security** check box 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.
- Step 25** Check the **Enable Storm Control** check box 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.
- Step 26** Check the **Protocol Tunnelling** check box 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.

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

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Chapter 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Step 28** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)

## 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.

Perform the following steps.

- Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.
- Step 2** For Core Type, choose **Ethernet**.
- Step 3** For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.

**Step 4** Check the **CE Present** check box.

**Step 5** Click **Next**.

The Interface Type window appears.

**Step 6** 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 7** 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 8** Choose a CE **Encapsulation** type.

The choices are:

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

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

**Step 9** 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 10** 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 11** 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 12** 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 13** 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 14** 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 15** Choose a **Port Type**.

The choices are:

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

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

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

- Step 18** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.

- Step 19** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 20** 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 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).



**Note** Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

- Step 24** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).

- Step 25** Check the **UNI Port Security** check box 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.

**Step 26** Check the **Enable Storm Control** check box 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.

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

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Chapter 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Step 28** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)

## 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.

Perform the following steps.

**Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.

**Step 2** For Core Type, choose **Ethernet**.

**Step 3** For Service Type, choose **Ethernet Relay Multipoint Service (ERMS)**.

**Step 4** Uncheck the **CE Present** check box.

**Step 5** Click **Next**.

The Interface Type window appears.

**Step 6** 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 7** 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 8** 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 9** Choose a CE **Encapsulation** type.

The choices are:

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

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

**Step 10** 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 11** 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 12** 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 13** 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 14** 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 15** Choose a **Port Type**.

The choices are:

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

**Step 16** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.**Step 17** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.**Step 18** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B ERMS (EVP-LAN) Service*.**Step 19** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 20** 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 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).

**Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).

**Note** Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.**Step 24** Check the **Filter BPDU** check box to specify that the UNI port should not process Layer 2 Bridge Protocol Data Units (BPDUs).**Step 25** Check the **UNI Port Security** check box 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.

- Step 26** Check the **Enable Storm Control** check box 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.
- Step 27** Click the **Next** button, if you want to enable template support for the policy.
- The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Chapter 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.
- Step 28** Click **Finish**.

**Note**

The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)

## 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.

Perform the following steps.

- Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.
- Step 2** For Core Type, choose **Ethernet**.
- Step 3** For Service Type, choose **Ethernet Multipoint Service (EMS)**.
- Step 4** Check the **CE Present** check box.
- Step 5** Click **Next**.
- The Interface Type window appears.
- Step 6** 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 7** 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 8** 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 9** 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 10** 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 11** 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 12** 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 13** 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 14** 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 15** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

**Step 16** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

- Step 17** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.
- Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 19** 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 20** 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. Prime Fulfillment 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 Cisco Prime Fulfillment 1.0, 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, Cisco Prime Fulfillment 1.0 uses 9216 in both cases.
  - For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.
- Step 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).
- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).
- 

**Note** Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.
- Step 24** Check the **UNI Port Security** check box 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.

**Step 25** Check the **Enable Storm Control** check box 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.

**Step 26** Check the **Protocol Tunnelling** check box 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.

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

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Chapter 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Step 28** Click **Finish**.



**Note**

The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)



## 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. Perform the following steps.

- 
- Step 1** In the Service Information window of the VPLS Policy Editor, choose **VPLS** for the Service Type.
- Step 2** For Core Type, choose **Ethernet**.
- Step 3** For Service Type, choose **Ethernet Multipoint Service (EMS)**.
- Step 4** Uncheck the **CE Present** check box.
- Step 5** Click **Next**.  
The Interface Type window appears.
- Step 6** 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 7** 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 8** 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 9** 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 10** 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 11** 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 12** 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 13** 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 14** 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 15** Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.
- Step 16** Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.
- Step 17** In the **PE/UNI Interface Description** field, enter an optional description, for example *Customer-B EMS (EP-LAN) Service*.
- Step 18** Check the **VLAN ID AutoPick** check box if you want Prime Fulfillment 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 19** 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 20** Enter the **System MTU** in bytes.  
The maximum transmission unit (MTU) size is configurable and optional. Prime Fulfillment 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. Prime Fulfillment 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, Prime Fulfillment uses 9216 in both cases.
  - For the 7600 SVI (interface VLAN), the MTU size is 1500-9216.
- Step 21** 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 Prime Fulfillment automatically assigns a MAC-based ACL on the customer facing UNI port, based on values you enter in **UNI MAC addresses** (below).
- Step 22** Enter a **Port-Based ACL Name** (if you checked the **Use Existing ACL Name** check box, as mentioned in the previous step).

**Note**

Prime Fulfillment 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 23** Check the **Disable CDP** check box if you want to disable the Cisco Discover Protocol (CDP) on the UNI port.

**Step 24** Check the **UNI Port Security** check box if you want to provision port security-related CLIs to the UNI port by controlling the MAC addresses that are allowed to go through the interface.

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

**Step 25** Check the **Enable Storm Control** check box 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.

**Step 26** Check the **Protocol Tunnelling** check box 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.

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

The Template Association window appears. In this window, you can enable template support and, optionally, associate templates and data files with the policy. For instructions about associating templates with policies and how to use the features in this window, see [Chapter 49, “Using Templates and Data Files with Policies and Service Requests.”](#) When you have completed setting up templates and data files for the policy, click **Finish** in the Template Association window to close it and return to the Policy Editor window.

**Step 28** Click **Finish**.



**Note**

---

The VC ID is mapped from the VPN ID. By default, Prime Fulfillment 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 [Chapter 3, “Setting Up Logical Inventory.”](#)

---