CHAPTER 8

Creating a FlexUNI/EVC Ethernet Policy

This chapter contains an overview of FlexUNI/EVC support in Cisco Prime Fulfillment 6.1, as well as the basic steps to create a FlexUNI/EVC Ethernet policy. It contains the following sections:

For information on creating FlexUNI/EVC Ethernet service requests, see Chapter 9, “Managing a FlexUNI/EVC Ethernet Service Request.”

Note For a general overview of FlexUNI/EVC support in Prime Fulfillment, see the chapter “Layer 2 Concepts” in the *Cisco Prime Fulfillment Theory of Operations Guide 6.1*.

Note For Ethernet (E-Line and E-LAN) services, use of the FlexUNI/EVC policy and service request is recommended. If you are provisioning services using the FlexUNI/EVC syntax, or plan to do so in the future, use the FlexUNI/EVC service. Existing services that have been provisioned using the L2VPN and VPLS service policy types are still supported and can be maintained with those service types. For ATM and FRoMPLS services, use the L2VPN service policy, as before.

Defining the FlexUNI/EVC Ethernet Policy

You must define a FlexUNI/EVC Ethernet policy before you can provision a service. A policy can be shared by one or more service requests that have similar service requirements.

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

An Editable check box in for an attribute in the policy gives the network operator the option of making a field editable. If the value is set to editable, the service request creator can change the value(s) of the particular policy attribute. If the value is *not* set to editable, the service request creator cannot change the attribute.

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.

To define a FlexUNI/EVC Ethernet policy, you start by setting the service type attributes. To do this, perform the following steps.

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

The Policy Manager window appears.

Step 2 Click **Create**.

Step 3 Choose **FlexUNI (EVC) Policy**.

The Service Information window appears.

Step 4 Enter a **Policy Name** for the FlexUNI/EVC policy.

Step 5 Choose the **Policy Owner** for the FlexUNI/EVC policy.

There are three types of FlexUNI/EVC policy ownership:

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

This ownership has relevance when the Prime Fulfillment Role-Based Access Control (RBAC) comes into play. For example, a FlexUNI/EVC 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 FlexUNI/EVC 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 **Policy Type**.

The choices are:

- **ETHERNET**
- **ATM-Ethernet Interworking**

Note This chapter describes creating the ETHERNET policy type. For information on using the FlexUNI/EVC ATM-Ethernet Interworking policy type, see Chapter 10, "Creating a FlexUNI/EVC ATM-Ethernet Interworking Policy."

Step 8 Click **Next**.

The Service Options window appears.

Step 9 Continue with the steps contained in the next section, Setting the Service Options, page 8-3.

Setting the Service Options

This section describes how to set the service options for the FlexUNI/EVC Ethernet policy,

To set the FlexUNI/EVC service options, perform the following steps.

Step 1 Check the **CE Directly Connected to FlexUNI** check box if the CEs are directly connected to the N-PE.

This check box is not checked by default.

Note 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 FlexUNI/EVC policy can modify the editable parameter during FlexUNI/EVC service request creation.

Usage notes:

- If the check box is checked, a service request created using this policy can have only directly connected links. No Ethernet access nodes will be involved.
- If the check box is unchecked, a service request created using this policy might or might not have Ethernet access nodes in the links.
- When a CE is directly connected to the N-PE, NPCs are not applicable to the link while creating service requests.
- When a CE is not directly connected to the N-PE, NPCs are used during service request creation, as per standard Prime Fulfillment behavior. There is no change in NPC implementation to support FlexUNI/EVC functionality.

Step 2 Check the **All Links Terminate on FlexUNI** check box if all links need to be configured with FlexUNI/EVC features.

This check box is not check by default. Usage notes:

- If the check box is checked, a service request created using such policy will have all links using the FlexUNI/EVC feature.
- If the check box is unchecked, zero or more links can use the FlexUNI/EVC feature. This ensures that existing platforms can still be used in one or more links while delivering the services. This allows the possibility of a link with FlexUNI/EVC support being added in the future.

  Note If the check box is unchecked, in the service request creation process the user must indicate whether or not the created link is FlexUNI or non-FlexUNI.

- If no links are expected to use the FlexUNI/EVC feature even in the future (for example, if the provider is not planning to upgrade to the EVC infrastructure for the service that is being created), existing Prime Fulfillment policy types (L2VPN or VPLS) can be used instead of FlexUNI/EVC.

Step 3 Choose an **MPLS Core Connectivity Type** from the drop-down list.

Note The core option supports MPLS only. There is no L2TPv3 support for this service.

The choices are:

- **PSEUDOWIRE**—Choose this option to allow connectivity between two N-PEs across the MPLS core. This option does not limit the service to point-to-point (E-Line). This is because even with the PSEUDOWIRE option selected, there can still be multiple CEs connected to a bridge domain on one or both sides of the pseudowire.
- **LOCAL**—Choose this option for local connect cases in which there is no connectivity required across the MPLS core.

  Local connect supports the following scenarios:

  - All interfaces on the N-PE are FlexUNI-capable and using the EVC infrastructure. This is configured by associating all of the customer traffic on these interfaces to a bridge domain. This consumes a VLAN ID on the N-PE (equal to the bridge domain ID).
  - Some interfaces on the N-PE are FlexUNI-capable, while others are switch-port-based. In such cases, all of the customer traffic on the interfaces that are configured with the EVC infrastructure are associated to a bridge domain. The traffic on the non-FlexUNI interfaces (and all the access nodes/interfaces beyond this N-PE) are configured with the Service Provider VLAN ID, where the Service Provider VLAN ID is the same as the bridge domain ID for the EVC-based services.
  - Only two interfaces on the N-PE are involved, and both are based on FlexUNI-capable line cards. In the first case, the operator might choose not to configure the bridge domain option. In this case, the **connect** command that is used for the local connects are used, and the global VLAN is conserved on the device. If the operator chooses to configure with the bridge domain option, both interfaces are associated to a bridge domain ID, so that additional local links can be added to the service in future. This consumes a VLAN ID (bridge domain ID) on the N-PE.
- **VPLS**—Choose this option to allow connectivity between multiple N-PEs across the MPLS core.

  There is no limit on the number of N-PEs across the MPLS core within a service request. However, many service requests can refer to the same customer-associated VPN.

Note Attributes available in subsequent windows of the policy workflow dynamically change based on the choice made for the MPLS Core Connectivity Type (PSEUDOWIRE, LOCAL, or VPLS). For completeness, all attributes available for the different core types are documented in the following steps. Attributes apply to all core types, unless otherwise noted.

Note Also, some attributes are supported only on IOS or IOS XR platforms. Attributes apply to both platforms, unless otherwise noted. All platform-specific attributes are visible in the policy workflow windows. Later, when a service request is created based on the policy (and specific devices are associated with the service request), platform-specific attributes are filtered from service request windows, depending on the device type (IOS or IOS XR).

Step 4 Check the **Configure With Bridge Domain** check box to determine bridge domain characteristics.

The behavior of the Configure With Bridge-Domain option works in tandem with the choice you selected in the MPLS Core Connectivity Type option, as follows.

- **PSEUDOWIRE** as the MPLS Core Connectivity Type. There are two cases:

  A. With FlexUNI:

  - If **Configure With Bridge Domain** is checked, the policy configures pseudowires under SVIs associated to the bridge domain.

- If **Configure With Bridge Domain** is unchecked, the policy will configure pseudowires directly under the service instance. This conserves the global VLAN.

B. Without FlexUNI:

- If **Configure With Bridge Domain** is checked, the policy configures pseudowires as in L2VPN services (with SVIs).
- If **Configure With Bridge Domain** is unchecked, the policy configures pseudowires directly under subinterfaces.

Only pseudowires can be either configured directly under service instance of the corresponding FlexUNI-capable interface or under SVIs associated to the bridge domain.

- **LOCAL** as the MPLS Core Connectivity Type:
  - If **Configure With Bridge Domain** is checked, the policy allows either point-to-point or multipoint local connect services.
  - If **Configure With Bridge Domain** is unchecked, Prime Fulfillment allows only point-to-point local connects without bridge domain.
- **VPLS—Configure With Bridge Domain** is checked by default and non-editable.

Step 5 Click **Next**.

The FlexUNI Attribute window appears.

Step 6 Continue with the steps contained in the next section, Setting the FlexUNI Attributes, page 8-5.

Setting the FlexUNI Attributes

This section describes how to set the FlexUNI attributes for the FlexUNI/EVC Ethernet policy.

FlexUNI attributes are organized under the following categories:.

- Service Attributes
- VLAN Match Criteria
- VLAN Rewrite Criteria

The following sections describe how to set the options under each category.

Setting the Service Attributes

To set the FlexUNI service attributes, perform the following steps.

Step 1 Check the **AutoPick Service Instance ID** check box to specify that the service instance ID will be autogenerated and allocated to the link during service request creation.

If the check box is unchecked, while setting the Prime Fulfillment link attributes during service request creation, Prime Fulfillment will prompt the operator to specify the service instance ID.

Usage notes:

- The service instance ID represents an Ethernet Flow Point (EFP) on an interface in the EVC infrastructure. The service instance ID is locally significant to the interface. This ID has to be unique only at the interface level. The ID must be a value from 1 to 8000.

- There are no resource pools available in Prime Fulfillment from which to allocate the service instance IDs.
- It is the responsibility of the operator creating the service request to maintain the uniqueness of the ID at the interface level.

Step 2 Check the **AutoPick Service Instance Name** check box to have Prime Fulfillment autogenerate a service instance name when you create a service request based on the policy. The autogenerated value is in the following pattern: *CustomerName_ServiceRequestJobID*.

If the check box is unchecked, then you can enter a value during service request creation.

Step 3 Check the **Enable PseudoWire Redundancy** check box to enable pseudowire redundancy (alternative termination device) under certain conditions.

Usage notes:

- Enable Pseudo Wire Redundancy is only available if the MPLS Core Connectivity Type was set as PSEUDOWIRE in the Service Options window (see Setting the Service Options, page 8-3).
- See Appendix E, "Terminating an Access Ring on Two N-PEs" and, specifically, the section Using N-PE Redundancy in FlexUNI/EVC Service Requests, page E-3, for notes on how this option can be used.

Step 4 Check the **AutoPick VC ID** check box to have Prime Fulfillment autopick the VC ID during service request creation.

If this check box is unchecked, the operator will be prompted to specify a VC ID during service request creation.

Usage notes:

- This attribute is available only if MPLS Core Connectivity of Type was set as PSEUDOWIRE or VPLS in the Service Options window (see Setting the Service Options, page 8-3).
- When AutoPick VC ID is checked, Prime Fulfillment allocates a VC ID for pseudowires from the Prime Fulfillment-managed VC ID resource pool.
- If MPLS Core Connectivity of Type is VPLS, Prime Fulfillment allocates the VPLS VPN ID from the Prime Fulfillment-managed VC ID resource pool.

Step 5 Check the **AutoPick Bridge Domain/VLAN ID** check box to have Prime Fulfillment autopick the VLAN ID for the service request during service request creation.

If this check box is unchecked, the operator will be prompted to specify a VLAN ID during service request creation.

Usage notes:

- AutoPick Bridge Domain/VLAN ID consumes a global VLAN ID on the device.
- The bridge domain/VLAN ID is picked from the existing Prime Fulfillment VLAN pool. Once the VLAN ID is assigned in the service request, Prime Fulfillment makes the VLAN ID unavailable for subsequent service requests.
- In the case of manual VLAN ID allocation, Prime Fulfillment does not manage the VLAN ID if the ID lies outside the range of an Prime Fulfillment-managed VLAN pool. In this case, the operator must ensure the uniqueness of the ID in the Ethernet access domain. If an operator specifies a VLAN ID that is within the range of an Prime Fulfillment-managed VLAN pool and the VLAN ID is already in use in the access domain, Prime Fulfillment displays an error message indicating that the VLAN ID is in use.

Note on Access VLAN IDs

An access VLAN ID is of local significance to the FlexUNI-capable ports. It should not be confused with the global VLANs. This can be visualized as a partitioning of the Ethernet access network beyond the FlexUNI ports into several subEthernet access domains (one each for a FlexUNI-capable port).

However, all the service interfaces on the Ethernet access nodes beyond the FlexUNI ports will have this very same VLAN ID for a link. This ID must be manually specified by the operator when setting the link attributes during service request creation. The operator must ensure the uniqueness of the ID across the FlexUNI-demarcated Ethernet access domain.

These VLAN IDs are not managed by Prime Fulfillment by means of locally-significant VLAN pools. But once a VLAN ID is assigned for a link in the service request, Prime Fulfillment makes the VLAN unavailable for subsequent service requests within the Ethernet access domain demarcated by the FlexUNI. Likewise, if a manually-specified VLAN is already in use in the access domain delimited by the FlexUNI, Prime Fulfillment will display an error message indicating that the new VLAN ID being specified is already in use on the NPC. The operator will be prompted to specify a different VLAN ID, which will be provisioned on the L2 access nodes.

Step 6 Check the **AutoPick Bridge Group Name** check box to have Prime Fulfillment autopick the group name for the service request during service request creation.

If this check box is unchecked, the operator will be prompted to specify a group name during service request creation. If the check box is checked, the group name will default to the customer name.

Note This attribute is applicable only for supported IOS XR devices.

Step 7 Check the **AutoPick Bridge Domain Name** check box to have Prime Fulfillment autopick the domain name for the service request during service request creation.

Usage notes:

- If this check box is unchecked, the operator will be prompted to specify a domain name during service request creation.
- If the check box is checked, the domain name will default to the following format:
  - For pseudowire and local connect core types: *ISC-Job-Job_ID*, where *Job_ID* is the service request job ID.
  - For VPLS core type: *ISC-VPN_Name-VPN_ID*, where *VPN_Name* is the name of the VPLS VPN being used, and *VPN_ID* is the VPN ID used in the service request.

Note This attribute is applicable only for supported IOS XR devices.

Step 8 Continue with the steps contained in the next section, Setting the VLAN Matching Criteria Attributes, page 8-7.

Setting the VLAN Matching Criteria Attributes

Prior to the introduction of the FlexUNI capability, service providers could either deploy service-multiplexed services (ERS/ERMS or EVPL/EVCS) or service-bundled services on a single port. Both could not be supported simultaneously due to the limitations in the infrastructure, which only allowed matching the outer-most VLAN tag.

One of the key benefits of FlexUNI/EVC support in Prime Fulfillment is to provide a flexible means to examine the VLAN tags (up to two levels) of the incoming frames and associate them to appropriate Ethernet Flow Points (EFPs). This allows service providers to deploy simultaneously both the service-multiplexed and service-bundled services on a single port.

To set the FlexUNI VLAN matching criteria attributes, perform the following steps.

Step 1 Check the **Both Tags** check box to enable service requests created with the policy to match both the inner and outer VLAN tags of the incoming frames.

If you do not check this check box, service requests created with the policy will match only the outer VLAN tag of the incoming frames.

Checking the Both Tags attribute causes the Inner VLAN Ranges attribute (covered in the next steps) to appear in the FlexUNI Attribute window.

Step 2 Check the **Inner VLAN Ranges** check box to enable the range of inner VLAN tags to be specified during service request creation.

If the check box is unchecked, the range of inner VLAN tags are not allowed. In this case, the operator must specify discrete VLAN IDs during service request creation.

Step 3 Check the **Outer VLAN Ranges** check box to enable the range of outer VLAN tags to be specified during service request creation.

If the check box is unchecked, the range of outer VLAN tags are not allowed. In this case, the operator must specify discrete VLAN IDs during service request creation.

Step 4 Continue with the steps contained in the next section, Setting the VLAN Rewrite Criteria Attributes, page 8-8.

Setting the VLAN Rewrite Criteria Attributes

Together with VLAN matching criteria, VLAN rewrite makes the FlexUNI/EVC infrastructure very powerful and flexible. The following VLAN rewrite options are supported:

- Pop one or two tags.
- Push one or two tags.
- Translation (1:1, 2:1, 1:2, 2:2).

Be aware of the following considerations when setting the VLAN rewrite criteria attributes:

- Only one kind of rewrite can be done on every CE-facing FlexUNI link.
- All VLAN rewrites are done using the **symmetric** keyword on the ingress traffic (for example, **rewrite ingress tag pop 2 symmetric**).
- For any service instance, only one type of rewrite option (pop, push, or translate) is allowed per instance. For example, if pop out is enabled, push inner, push outer, translate inner, and translate outer are not available.

To set the FlexUNI VLAN rewrite criteria attributes, perform the following steps.

Step 1 Check the **Pop Outer** check box to pop the outer VLAN ID tag of the incoming frames that fulfill the match criteria.

If this check box is unchecked, the outer tag of the incoming traffic is not popped.

Step 2 Check the **Pop Inner** check box to pop the inner VLAN ID tag of the incoming frames that fulfill the match-criteria.

If this check box is unchecked, the inner tag is not popped. Note that, if Pop Inner is checked, Pop Outer is automatically checked.

Step 3 Check the **Push Outer** check box to impose an outer VLAN ID tag onto the incoming frames that fulfill the match criteria.

If this check box is unchecked, no outer tag is imposed on the incoming frames.

Usage notes:

- If Push Outer is checked, all service requests created with the policy push a dot1q outer tag on the incoming frames matching the match criteria. When creating the link during service creation, the operator can specify an outer tag with a value from 1 to 4096.
- This attribute is available regardless of the number of tags used in the match criteria. Whether the incoming traffic is double tagged or single tagged, if Push Outer is enabled, all corresponding service requests push an outer tag. All subsequent nodes consider only the outer-most two tags (if FlexUNI-capable) or just one tag (not FlexUNI-capable) and treat the inner-most tags transparently as payload.
- This VLAN ID is not derived from Prime Fulfillment-managed VLAN ID pools.

Step 4 Check the **Push Inner** check box to impose an inner VLAN ID tag onto the incoming frames that fulfill the match criteria.

This operation pushes both an inner and an outer tag onto the incoming packet, not just an inner tag. If this check box is unchecked, no inner tag is imposed on the incoming frames.

Usage notes:

- If Push Inner is checked, all service requests created with the policy push a dot1q inner tag on the incoming frames matching the match criteria. When creating the link during service creation, the operator can specify an inner tag with a value from 1 to 4096.
- If Push Inner is checked, Push Outer is automatically checked.
- This attribute is available regardless of the number of tags used in the match criteria. Regardless of whether the incoming traffic is double tagged or single tagged, if Push Inner is enabled, all corresponding service requests push an inner tag. All subsequent nodes consider only the outer-most two tags (if FlexUNI-capable) or just one tag (not FlexUNI-capable) and treat the inner-most tags transparently as payload.
- This VLAN ID is not derived from Prime Fulfillment-managed VLAN ID pools.

Step 5 Check the **Translate Outer** check box to allow the operator to specify a target outer VLAN ID during service request creation.

The outer tag of all the incoming frames that fulfill the match criteria are translated to this ID. If the check box is unchecked, no outer tag translation is performed. See Table 8-1.

Step 6 Check the **Translate Inner** check box to allow the operator to specify a target inner VLAN ID during service request creation.

The inner tag of all the incoming frames that fulfill the match criteria are translated to this ID. If the check box is unchecked, no inner tag translation is performed. See Table 8-1.

Note Table 8-1 summarizes the realization of different VLAN translations available in the FlexUNI/EVC infrastructure. The second and third columns (Match Outer Tag and Match Inner Tag) refer to policy settings. The last two columns (Translate Outer Tag and Translate Inner Tag) indicate the VLAN translation that occurs on the incoming frames.

Table 8-1 VLAN Translation Summary Table

Type	Match Outer Tag	Match Inner Tag	Translate Outer Tag	Translate Inner Tag
1:1	True	N/A	Yes	No
1:2	True	N/A	Yes	Yes
2:1	True	True	Yes	No
2:2	True	True	Yes	Yes

Step 7 Click **Next**.

The Interface Attribute window appears.

Step 8 Continue with the steps contained in the next section, Setting the Interface Attributes, page 8-10.

Setting the Interface Attributes

This step of creating the FlexUNI/EVC Ethernet policy involves setting the interface attributes in the Interface Attribute window. The attributes you can configure in this window are grouped under the following categories:

- N-PE/U-PE information
- Speed and duplex information
- ACL name and MAC addresses
- UNI port security
- Storm control
- L2 protocol tunneling

In some cases, checking an attribute causes additional attributes to appear in the GUI. This is covered in the steps that follow.

Note If the CE is directly connected to an N-PE, only speed, duplex, UNI shutdown, and other generic options are presented. In this case, port security, storm control, L2 protocol tunneling, and other advanced features are not supported due to the current platform limitations. If these features are needed for a service, the service provider must deploy Layer 2 Ethernet access nodes beyond the FlexUNI to support these requirements.

Note Attributes available in the Interface Attributes window dynamically change based on the choice made for the MPLS Core Connectivity Type (PSEUDOWIRE, LOCAL, or VPLS) in the Service Options window (see Setting the Service Options, page 8-3). For completeness, all attributes available for the different core types are documented in the following steps. Attributes apply to all core types, unless otherwise noted.

To set the FlexUNI/EVC interface attributes, perform the following steps.

Step 1 Choose an **Encapsulation** type.

The choices are:

- **DOT1QTRUNK**—Configures the UNI as a trunk with 802.1q encapsulation. If the UNI belongs to a directly connected and FlexUNI link, this setting signifies that the incoming frames are 802.1q encapsulated and that they match the VLAN ID configured for the link. This specific topology does not involve a trunk UNI as such.
- **DOT1QTUNNEL**—Configures the UNI as an 802.1q tunnel (also known as a dot1q tunnel or Q-in-Q) port.
- **ACCESS**—Configures the UNI as an access port.

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

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

Step 3 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 4 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, in order to support modification on a per-service request basis.

Step 5 Enter a **Link Media** (optional) of None, auto-select, rj45, or sfp.

Step 6 Enter a **Link Speed** (optional) of None, 10, 100, 1000, Auto, or nonegotiate.

Step 7 Enter a **Link Duplex** (optional) of None, Full, Half, or Auto.

Step 8 Check the **Use Existing ACL Name** check box if you want to 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 9 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 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 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 12 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 13 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 choose, enter the shutdown threshold and drop threshold for that protocol:

a. **Enable cdp**—Enable Layer 2 tunnelling on Cisco Discover Protocol (CDP).

b. **cdp shutdown threshold—**Enter the number of packets per second to be received before the interface is shut down.

c. **cdp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping CDP packets.

d. **Enable vtp**—Enable Layer 2 tunnelling on VLAN Trunk Protocol (VTP).

e. **vtp shutdown threshold**—Enter the number of packets per second to be received before the interface is shut down.

f. **vtp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping VTP packets.

g. **Enable stp—**Enable Layer 2 tunnelling on Spanning Tree Protocol (STP).

h. **stp shutdown threshold—**Enter the number of packets per second to be received before the interface is shut down.

i. **stp drop threshold**—Enter the number of packets per second to be received at which point the interface will start dropping STP packets.

j. **Recovery Interval**—Enter the amount of time, in seconds, to wait before recovering a UNI port.

Step 14 Check the **N-PE Pseudo-wire on SVI** check box to have Prime Fulfillment generate forwarding commands under SVIs (switch virtual interfaces).

By default, this check box is not checked. In this case, Prime Fulfillment generates forwarding commands under the service instance.

For a FlexUNI link, the attribute N-PE Pseudo-wire on SVI is dependent on the value of the attribute Configure with Bridge Domain (this is available in the policy workflow in the EVC Policy Editor - Service Options window). N-PE Pseudo-wire on SVI, if enabled, will be reflected only when Configure with Bridge Domain is set to true. Otherwise, the service request will not be created with xconnect under SVI, even if N-PE Pseudo-wire on SVI is enabled.

Usage notes:

- Prime Fulfillment supports a hybrid configuration for FlexUNI/EVC service requests. In a hybrid configuration, the forwarding commands (such as xconnect) for one side of an attachment circuit can be configured under a service instance, and the xconnect configuration for the other side of the attachment circuit can be configured under a switch virtual interface (SVI).
- For examples of these cases, see configlet examples FlexUNI/EVC (Pseudowire Core Connectivity, Bridge Domain, Pseudowire on SVI), page 18-39 and FlexUNI/EVC (Pseudowire Core Connectivity, no Bridge Domain, no Pseudowire on SVI), page 18-40.
- N-PE Pseudo-wire on SVI is applicable for all connectivity types (PSEUDOWIRE, VPLS, and LOCAL), but a hybrid SVI configuration is possible only for pseudowire connectivity.
- When MPLS Core Connectivity Type is set as VPLS, the N-PE Pseudo-wire on SVI attribute is always enabled in the policy and service request.
- When MPLS Core Connectivity Type is set as LOCAL connectivity type, the N-PE Pseudo-wire on SVI attribute is always disabled in the policy and service request.
- The N-PE Pseudo-wire on SVI attribute is not supported for IOS XR devices. Only subinterfaces are supported on ASR 9000 devices; service instance is not supported. All the xconnect commands are configured on L2 subinterfaces.
- Table 8-2 shows various use cases for hybrid configuration for FlexUNI/EVC service requests.

Table 8-2 Use Cases for Hybrid Configuration for FlexUNI /EVC Service Requests

Use Bridge Domain	FlexUNI	N-PE Pseudowire on SVI	CLIs Generated
True	True	True	• xconnect under VLAN interface. • Service instance under main interface.
True	True	False	• xconnect under service instance. • Service instance under main interface.
False	True	N/A	• xconnect under service instance. • Service instance under main interface.
True	False	True	xconnect under VLAN interface.
True	False	False	xconnect under subinterface.
False	False	False	xconnect under subinterface.

Step 15 Specify the type of **VLAN Translation** for this policy by clicking the appropriate radio button.

The choices are:

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

Note For detailed coverage of setting up VLAN translation, see Chapter 19, "Setting Up VLAN Translation."

Note VLAN translation is only supported on links that are specified as non-FlexUNI at the service request level.

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

The maximum transmission unit (MTU) size is configurable and optional. The default size is 9216, and the range is 1500 to 9216. 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 to 1546.
- For the Cisco 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 to 9216. However, Cisco Prime Fulfillment 1.0 uses 9216 in both cases.
- For the Cisco 7600 SVI (interface VLAN), the MTU size is 1500 to 9216.

Step 17 Check the **PW Tunnel Selection** check box if you want to be able to manually select the Traffic Engineering (TE) tunnel for the pseudowire connecting point-to-point N-PEs.

This attribute is unchecked by default.

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

Step 18 Check the **Use PseudoWireClass** check box to enable the selection of a pseudowire class.

This attribute is unchecked by default.

Usage notes:

- The pseudowire class name is used for provisioning pw-class commands on IOS XR devices. See Creating and Modifying Pseudowire Classes for IOS XR Devices, page 7-10 for additional information on pseudowire class support for IOS XR devices.
- If **Use PseudoWireClass** is checked, an additional attribute, **PseudoWireClass**, appears in the GUI. Click the **Select** button of PseudoWireClass attribute to choose a pseudowire class previously created in Prime Fulfillment.

- The Use PseudoWireClass attribute is only available if the MPLS core connectivity type was set as PSEUDOWIRE in the Service Options window (see Setting the Service Options, page 8-3).
- Use PseudoWireClass is only applicable for IOS XR devices.

Step 19 For **L2VPN Group Name** choose one of the following from the drop-down list:

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

Usage notes:

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

Note The choices in the drop-down list are derived from a configurable DCPL property. For information about how to define the L2VPN Group Name choices available in the drop-down list, see Defining L2VPN Group Names for IOS XR Devices, page 7-13.

- The L2VPN Group Name attribute is not available if the MPLS core connectivity type was set as VPLS in the Service Options window (see Setting the Service Options, page 8-3).
- L2VPN Group Name is only applicable for IOS XR devices.

Step 20 Enter an **E-Line Name** to specify the point-to-point (p2p) E-line name.

Usage notes:

- If no value is specified for the **E-Line Name** in either the policy or the service request based on the policy, Prime Fulfillment autogenerates a default name as follows:
  - For PSEUDOWIRE core connectivity type, the format is:

    DeviceName--VC_ID
  - For LOCAL core connectivity type, the format is:

    DeviceName--0--VLAN_ID

  If the default name is more than 32 characters, the device names are truncated.
- The E-Line Name attribute is not available if the MPLS core connectivity type was set as VPLS in the Service Options window (see Setting the Service Options, page 8-3).
- E-Line Name is only applicable for IOS XR devices.

Step 21 If you would like to enable template association for this policy, click the **Next** button.

See the section Enabling Template Association, page 8-15 for information about this feature.

Step 22 To save the FlexUNI/EVC policy, click **Finish**.

To create a service request based on a FlexUNI/EVC policy, see Chapter 9, “Managing a FlexUNI/EVC Ethernet Service Request.”

Enabling Template Association

The Prime Fulfillment template feature gives you a means to download free-format CLIs to a device. If you enable templates, you can create templates and data files to download commands that are not currently supported by Prime Fulfillment.

Step 1 To enable template association for the policy, click the **Next** button in the Interface Attribute window (before clicking **Finish**).

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".

Step 2 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 3 To save the FlexUNI/EVC policy, click **Finish**.

To create a service request based on a FlexUNI/EVC policy, see Chapter 9, "Managing a FlexUNI/EVC Ethernet Service Request."