
# Creating an L2TPv3 Policy

This chapter contains the basic steps to create an L2TPv3 policy. It contains the following sections:



## Defining an L2TPv3 Policy

You must define an L2TPv3 policy before you can provision a Cisco IP Solution Center (ISC) L2TPv3-based L2VPN service. An L2TPv3 policy defines the common characteristics shared by the end-to-end wire attributes and 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.

The two major categories of an L2TPv3 policy correspond to the two major services that L2TPv3 provides:

- Frame Relay transport over L2TPv3, both port-based and DLCI-based MFR support.
- ATM transport over L2TPv3, VP mode and VC mode, single cell.

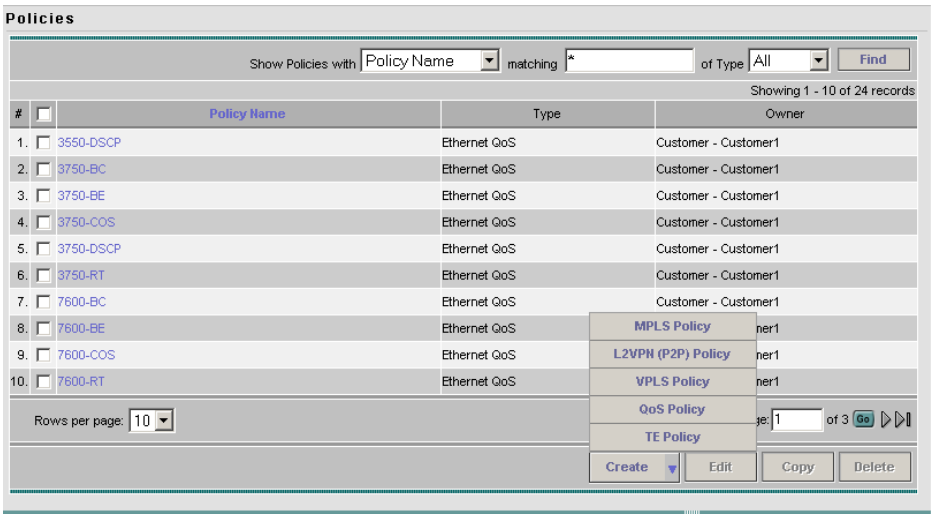
A policy is a template of most of the parameters needed to define an L2TPv3 service request. After you define it, an L2TPv3 policy can be used by all the L2TPv3 service requests that share a common set of characteristics.

You create a new L2TPv3 policy whenever you create a new type of service or a service with different parameters. L2TPv3 policy creation is normally performed by experienced network engineers.

To define an L2TPv3 policy in ISC, perform the following steps.

**Step 1** Select **Service Design** > **Policies**. The Policies window appears as shown in Figure 6-1.

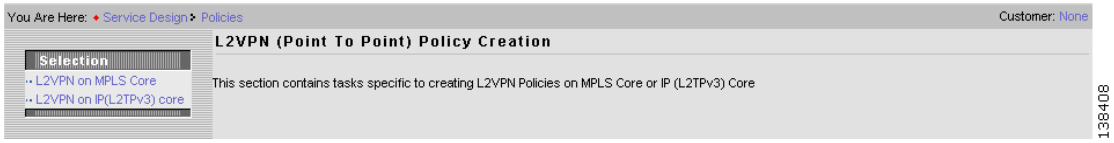
***Figure 6-1 Creating an L2TPv3 Policy***




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

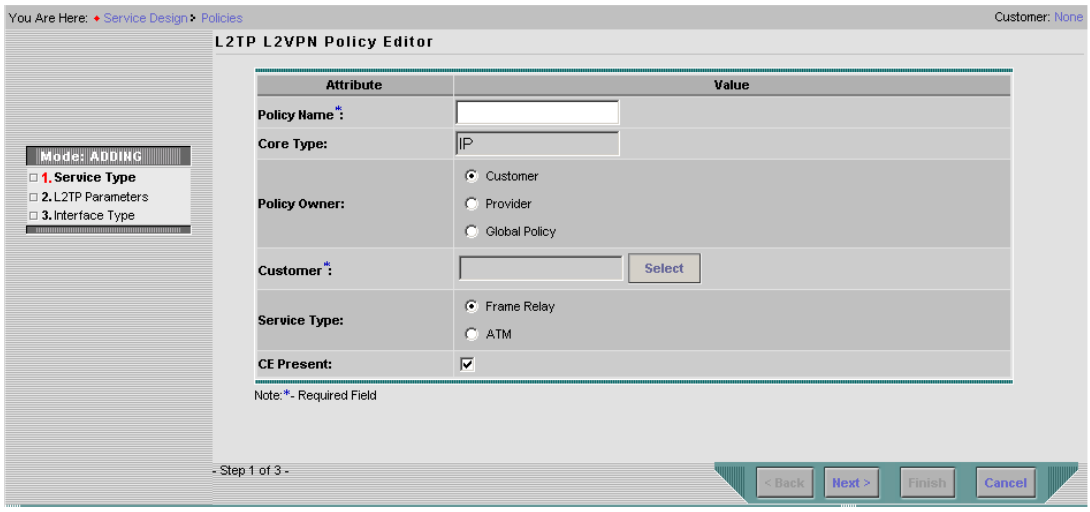
**Step 3** Select **L2VPN (P2P) Policy**. When you select L2VPN (P2P) Policy, the window in Figure 6-2 appears.

***Figure 6-2 L2VPN Policy Window***




**Step 4** Select **L2VPN on IP (L2TPv3) core**. The window in Figure 6-3 appears.

*Figure 6-3 L2TP L2VPN Policy Editor*




**Step 5** Enter a **Policy Name** for the L2TPv3 policy.

**Step 6** Choose the **Policy Owner** for the L2TPv3 policy.

There are three types of L2TPv3 policy ownership:

- Customer ownership
- Provider ownership
- Global ownership—Any service operator can make use of this L2TPv3 policy.

This ownership has relevance when the ISC Role-Based Access Control (RBAC) comes into play. For example, an L2TPv3 policy that is customer-owned can only be seen by operators who are allowed to work on this customer-owned policy.

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

**Step 7** Click **Select** to choose the owner of the L2TPv3 policy. (If you choose Global ownership, the Select function is not available.) The Select Customer window or the Select Provider window appears and you can choose an owner of the policy and click **Select**.

**Step 8** Choose the **Service Type** of the L2TPv3 policy.

There are two service types for L2TPv3 policies:

- **Frame Relay**
- **ATM**

**Step 9** Select the **CE Present** check box if you want ISC to ask the service operator who uses this L2TPv3 policy to provide a CE router and interface during service activation. The default is CE present in the service.

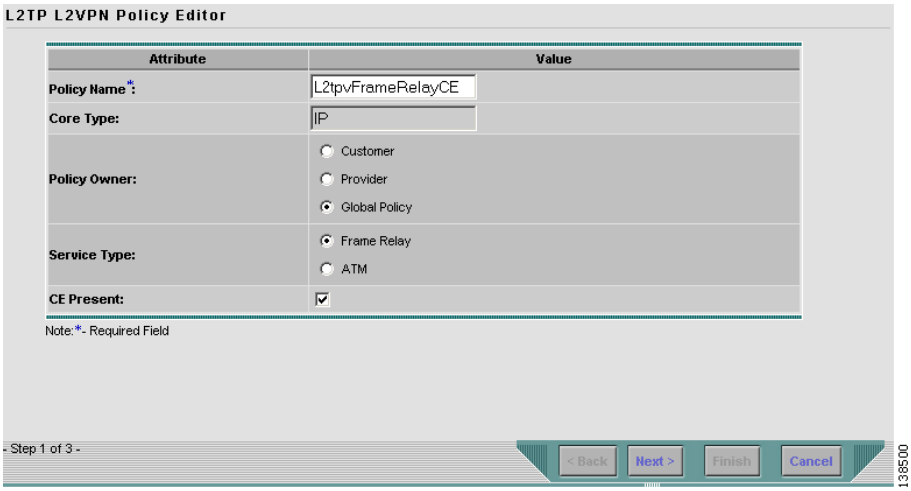
If you do not select the **CE Present** check box, ISC asks the service operator, during service activation, only for the PE router and customer-facing interface.

**Step 10** Click **Next**.

# Defining a Frame Relay Policy with a CE

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

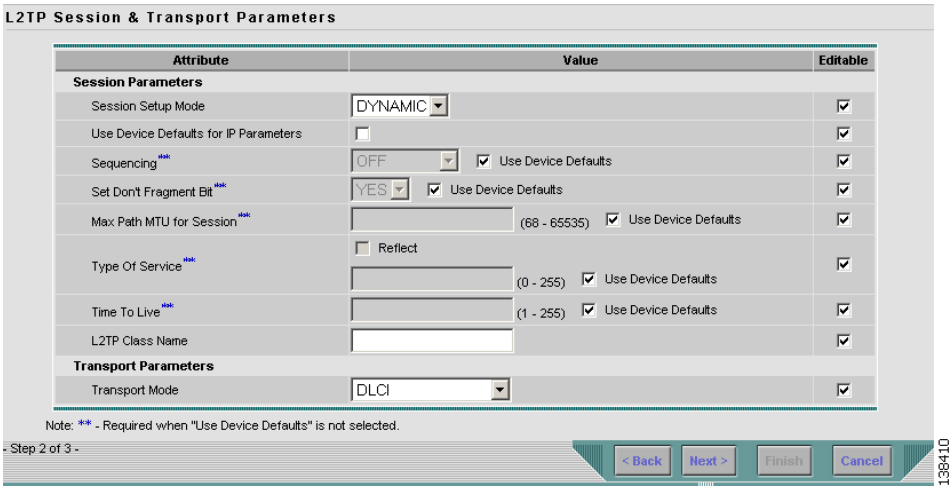
***Figure 6-4 Frame Relay Policy with a CE***




**Step 1** Click **Next**. The window in Figure 6-5 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

***Figure 6-5 Frame Relay Policy with a CE Attributes***



**Step 2** Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

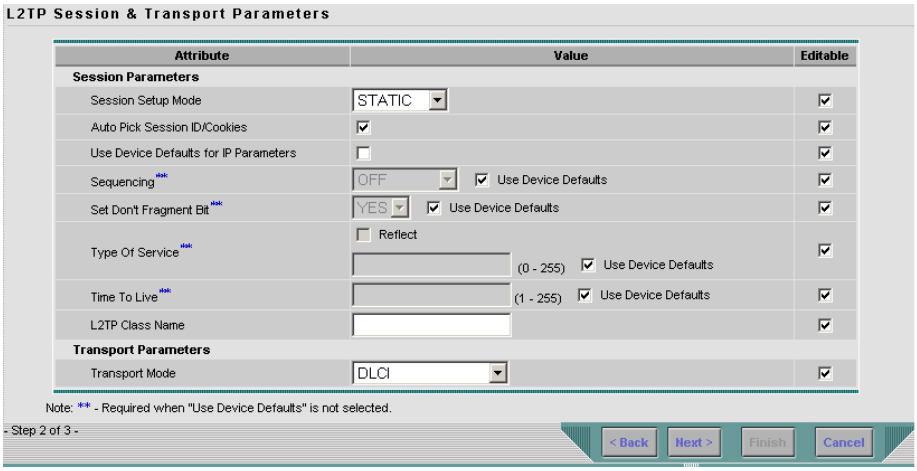
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-6. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

***Figure 6-6 Static Session Setup Mode***




**Step 3** Select the **Use Device Defaults for IP Parameters** check box if you do **not** want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

**Step 4** Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default**)**
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

**Step 5** **Set Don't Fragment Bit.** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudo wire.

**Step 6** **Max Path MTU for Session.** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535.

**Step 7** **Type Of Service (ToS).** Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers. Enter the ToS byte value used by all packets sent across the pseudo wire. The range is 0 to 255.

**Step 8** **Time To Live** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

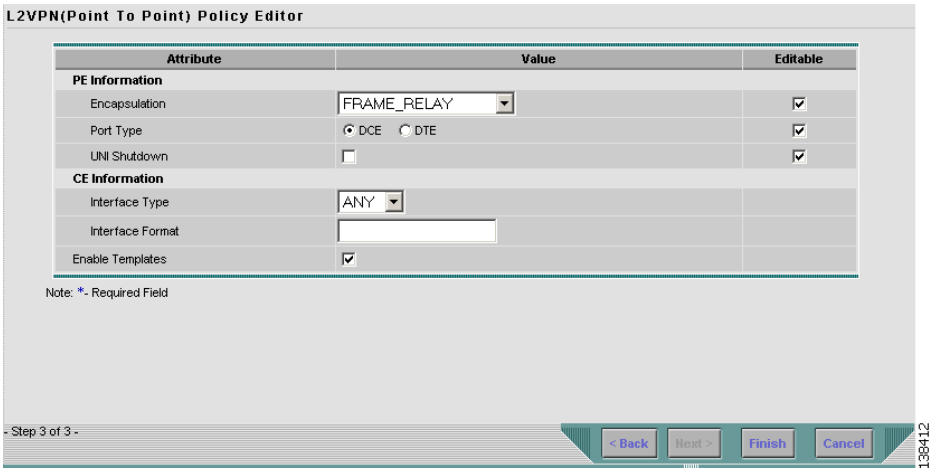
**Step 9** **L2TP Class Name** Enter a unique L2TP class name if you want to configure multiple L2TP classes. You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel.

**Step 10** Select the **Transport Mode** from the drop-down list. The choices are:

- **DLCI (**data-link connection identifier) is the default.
- **PORT_TRUNKING**

**Step 11** Click **Next**. The window in Figure 6-7 appears.

***Figure 6-7 Frame Relay Interface with a CE Attributes***




**Step 12** Choose the PE **Encapsulation** type. The choices are:

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

**Step 13** Choose the PE **Port Type**. The choices are:

- **DCE** (data circuit-terminating equipment)
- **DTE** (data terminal equipment)

For **DCLI** transport mode, set BOTH PEs to DCE or BOTH to DTE. If the PE setting is DCE, then ISC provisions the corresponding CE (if there is one) to be DTE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

For **PORT_TRUNKING** transport mode, set one PE to DTE and the other PE to DCE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

**Step 14** Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

**Step 15** Choose the CE **Interface Type.** The choices are:

- **ANY**

- **Serial**
- **MFR** (Multilink Frame Relay)
- **POS**

**Step 16** Enter the CE **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).

**Step 17** Choose the CE **Encapsulation** type. The choices are:

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

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

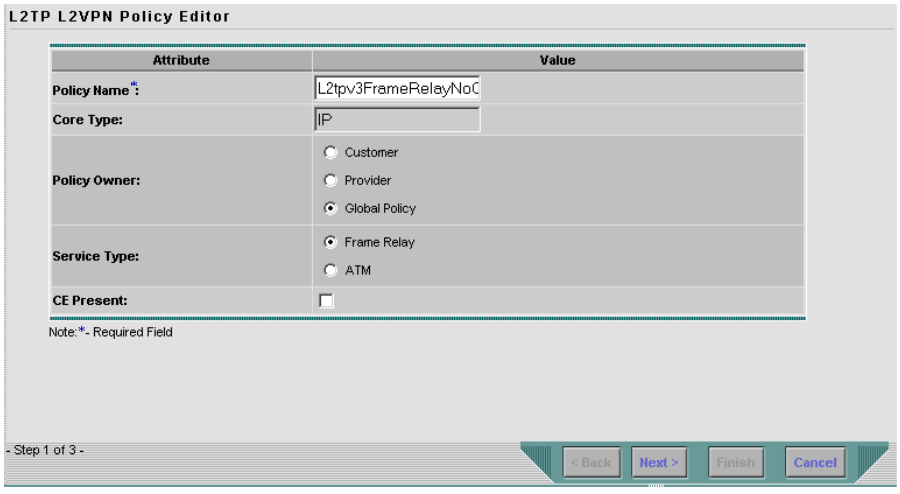
**Step 18** Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

**Step 19** Click **Finish**.

# Defining a Frame Relay Policy without a CE

This section describes defining an L2TPv3 Frame Relay policy without a CE present. Figure 6-8 is an example of the first page of this policy.

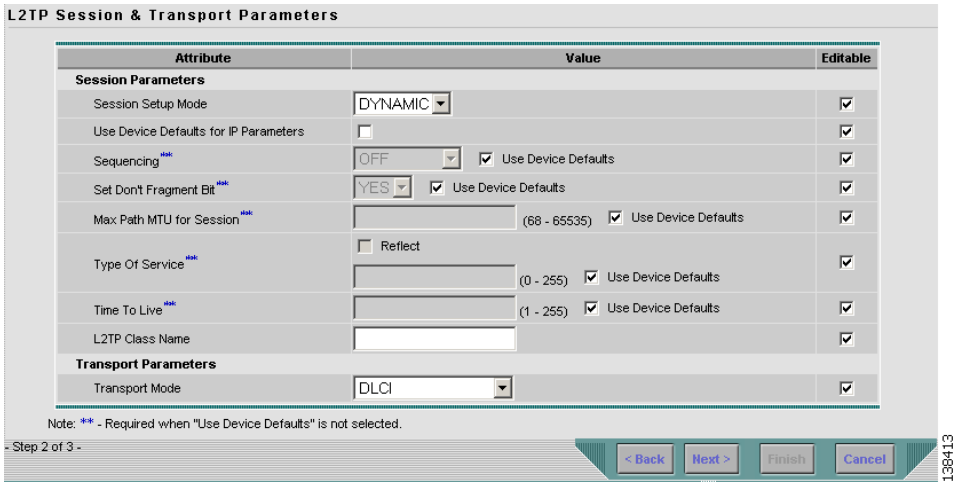
***Figure 6-8 Frame Relay Policy without a CE***




**Step 1** Click **Next**. The window in Figure 6-9 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

***Figure 6-9 Frame Relay without CE Policy Attributes***




**Step 2** Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

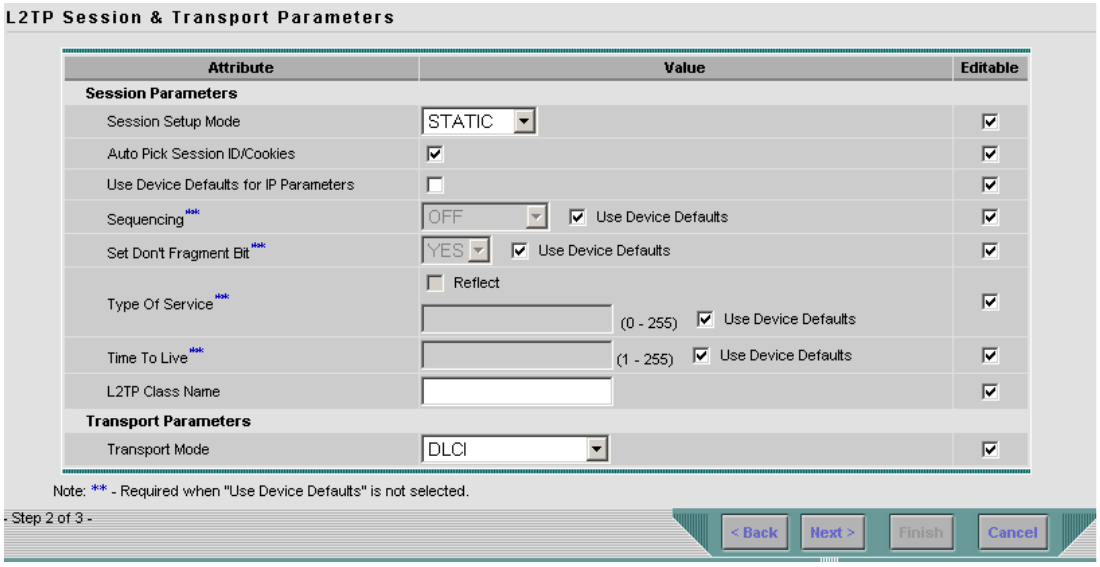
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-10. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

*Figure 6-10 Static Session Setup Mode*




**Step 3** Select the **Use Device Defaults for IP Parameters** check box if you do not want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

**Step 4** Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default**)**
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

**Step 5** **Set Don't Fragment Bit.** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudo wire.

**Step 6** **Max Path MTU for Session.** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535

**Step 7** **Type Of Service (ToS).** Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers. Enter the ToS byte value used by all packets sent across the pseudo wire. The range is 0 to 255.

**Step 8** **Time To Live** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

**Step 9** **L2TP Class Name** Enter a unique L2TP class name if you want to configure multiple L2TP classes.

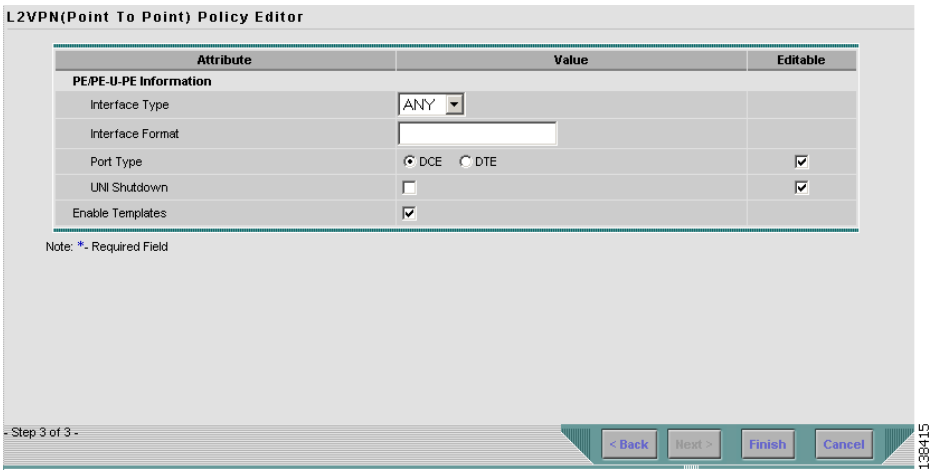
You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel.

**Step 10** Select the **Transport Mode** from the drop-down list. The choices are:

- **DLCI (**data-link connection identifier) is the default.
- **Port-trunking**

**Step 11** Click **Next**. The window in Figure 6-11 appears.

*Figure 6-11 PE Frame Relay without a CE*




**Step 12** Choose the PE **Interface Type**. The choices are:

- **ANY**
- **Serial**
- **MFR** (Multilink Frame Relay)
- **POS**

**Step 13** Enter the PE **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).

**Step 14** Choose the PE **Port Type**. The choices are:

- **DCE** (data circuit-terminating equipment)
- **DTE** (data terminal equipment)

For **DCLI** transport mode, set BOTH PEs to DCE or BOTH to DTE. If the PE setting is DCE, then ISC provisions the corresponding CE (if there is one) to be DTE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

For **PORT_TRUNKING** transport mode, set one PE to DTE and the other PE to DCE. If the PE setting is DTE, then ISC provisions the CE (if there is one) to be DCE.

**Step 15** Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

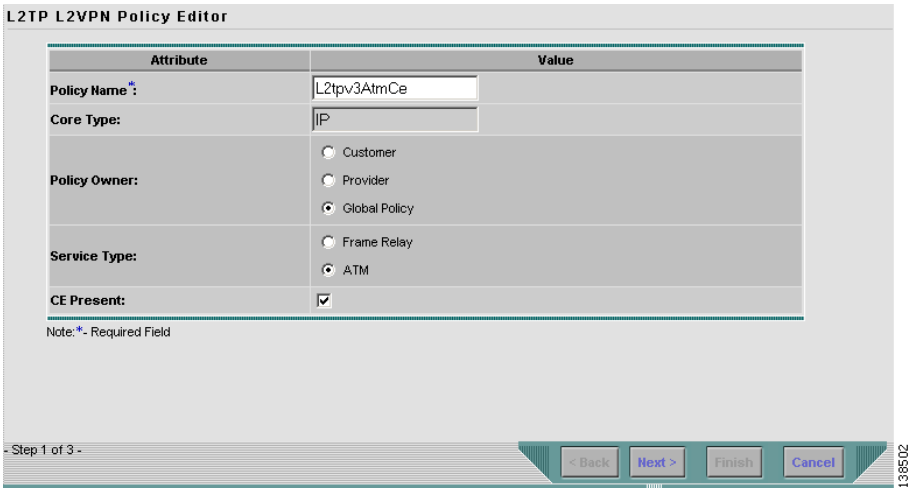
**Step 16** Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

**Step 17** Click **Finish**.

# Defining an ATM Policy with aCE

This section describes how to define an L2TPv3 ATM policy with CE present. Figure 6-12 is an example of the first page of this policy.

***Figure 6-12 ATM Policy with a CE***

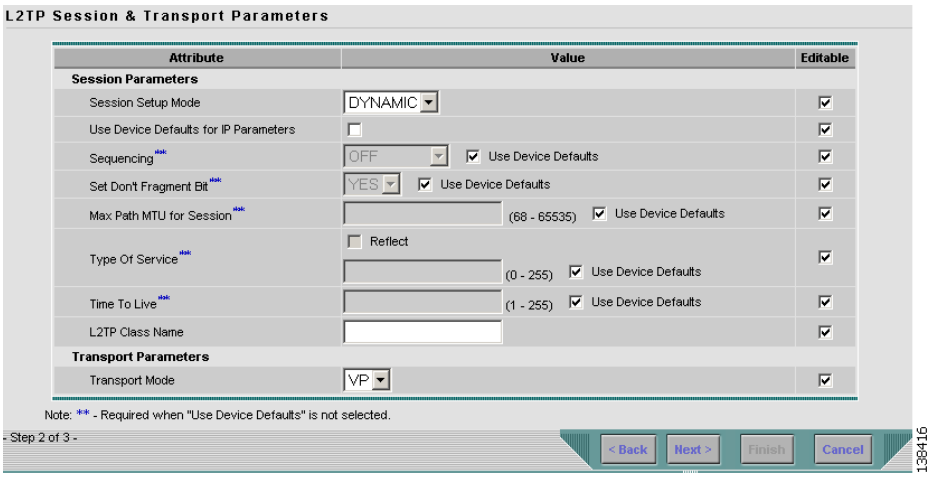



Perform the following steps.

**Step 1** Click **Next**. The window in Figure 6-13 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

***Figure 6-13 ATM Policy with CE Attributes***



**Step 2** Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

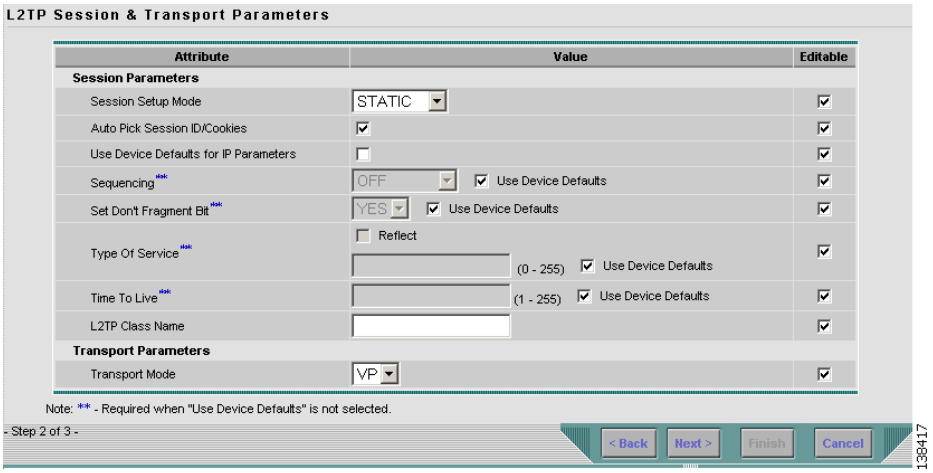
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-14. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

***Figure 6-14 Static Session Setup Mode***




**Step 3** Select the **Use Device Defaults for IP Parameters** check box if you do not want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

**Step 4** Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default**)**
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

**Step 5** **Set Don't Fragment Bit.** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudo wire.

**Step 6** **Max Path MTU for Session.** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535

**Step 7** **Type Of Service (ToS).** Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers. Enter the ToS byte value used by all packets sent across the pseudo wire. The range is 0 to 255.

**Step 8** **Time To Live.** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

**Step 9** **L2TP Class Name.** Enter a unique L2TP class name if you want to configure multiple L2TP classes.

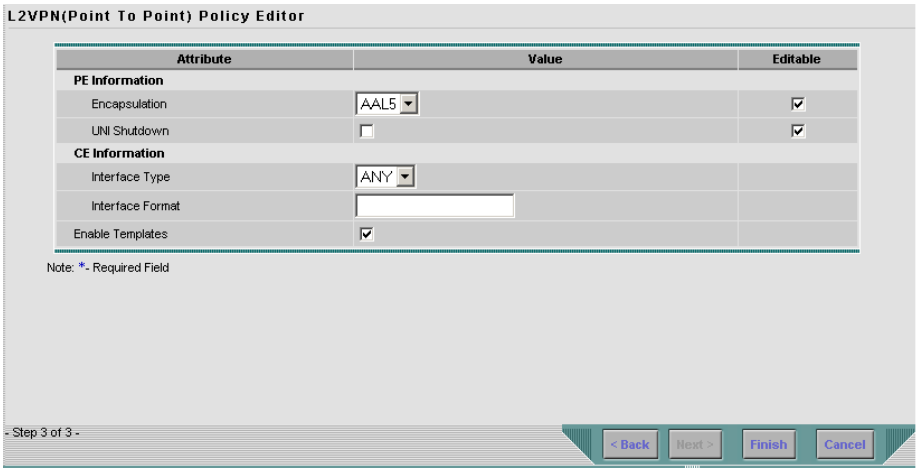
You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel. For ATM, the vpi/vci pair for CE must match the vpi/vci pair for PE.

**Step 10** Select the **Transport Mode** from the drop-down list. The choices are:

- **VP** (Virtual Path)
- **VC** (Virtual Circuit) This is the default.

**Step 11** Click **Next**. The window in Figure 6-15 appears.

***Figure 6-15 ATM with a CE Policy Attributes***




**Step 12** Choose the PE **Encapsulation** type from the drop-down list. The choices are:

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

**Step 13** Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

**Step 14** Choose the CE **Interface Type** from the drop-down list. The choices are:

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

**Step 15** Enter the CE **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 16** Choose the CE **Encapsulation Type** from the drop-down list. The choices are:

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

**Note** The CE Encapsulation Type only appears if you chose the CE Interface Type as ATM instead of ANY.

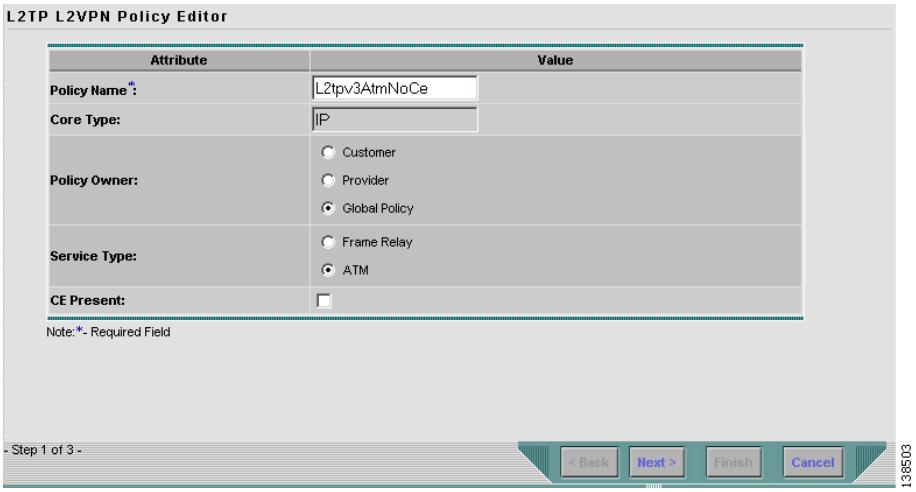
**Step 17** Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

**Step 18** Click **Finish**.

# Defining an ATM Policy without a CE

This section describes defining an ATM policy without a CE present. Figure 6-16 is an example of the first page of this policy.

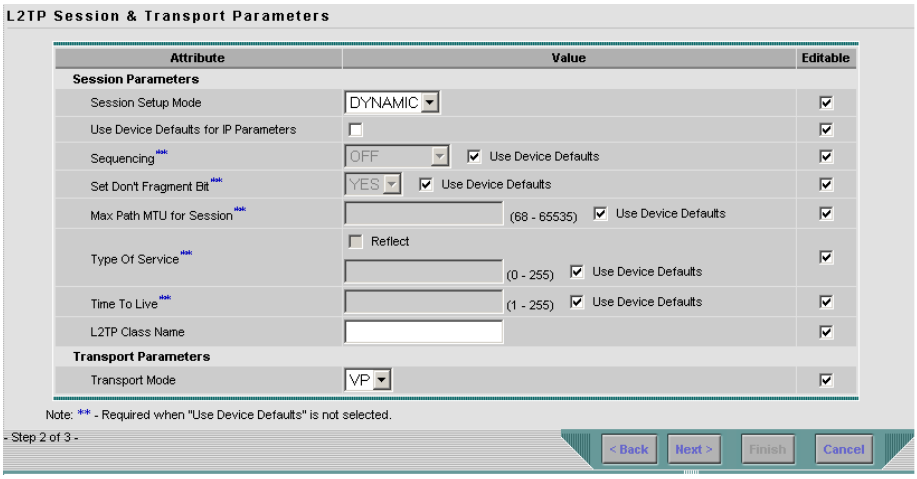
***Figure 6-16 ATM Policy without a CE***




**Step 1** Click **Next**. The window in Figure 6-17 appears.

The **Editable** check box gives you the option of making a field editable. If you select the **Editable** check box, the service operator who is using this L2TPv3 policy can modify the editable parameter during L2TPv3 service request creation.

*Figure 6-17 ATM without a CE Policy Attributes*




**Step 2** Choose the **Session Setup Mode** from the drop-down list. The choices are:

- **Dynamic** if you want to let the IOS control panel set up the session.

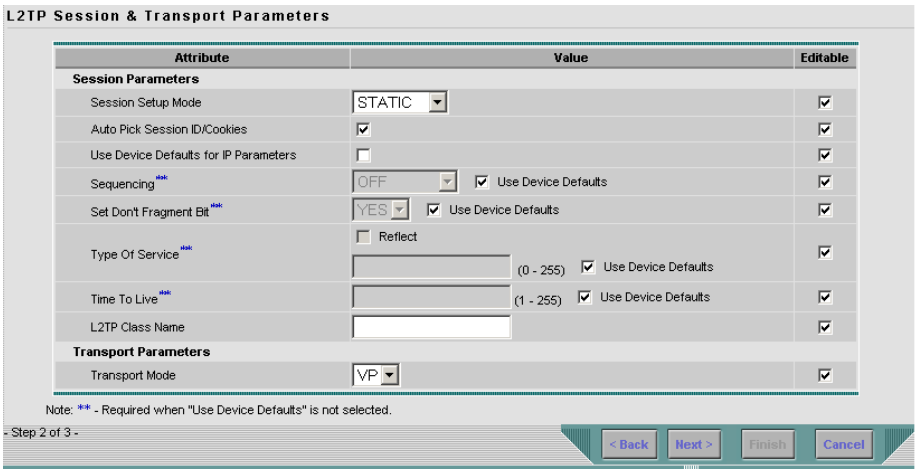
  We recommend Dynamic.

- **Static** if you want to manually setup a session by providing:
  - 2 session IDs
  - session cookies (for authentication purposes)
  - ISC provides auto-pick option for this mode

  Static L2TPv3 sessions for a PE router configure fixed values for the fields in the L2TP data header. A static L2TPv3 session allows the PE to tunnel Layer 2 traffic as soon as the end-to-end wire to which the session is bound comes up.

  If you choose **Static**, the **Auto Pick Session ID/Cookies** check box will appear. See Figure 6-18. If you do not select the **Auto Pick Session ID/Cookies** check box, ISC will require you to enter the size of the local cookie in bytes and the Session ID when you create a service request for this policy.

*Figure 6-18 Static Session Setup Mode*



**Step 3** Select the **Use Device Defaults for IP Parameters** check box if you do not want to see any of the fields for the pseudo-wire class. It is the default. Do not select this check box if you want to choose a device (that is, not use the default) for any of the following fields.

**Step 4** Select the direction in which **Sequencing** is enabled for data packets from the drop-down list. Select the check box if you want the default (**OFF**) for this field. The choices are:

- **OFF** (default**)**
- **TRANSMIT**
- **RECEIVE**
- **BOTH**

**Step 5** **Set Don't Fragment Bit** Choose **YES** to set the Don't Fragment Bit. Choose **NO** allow IP traffic from the CE router to be fragmented before the data enters the pseudowire.

**Step 6** **Max Path MTU for Session** Specify the maximum packet size, in bytes, that a particular interface can handle. The range is 68 to 65535

**Step 7** Type Of Service (ToS)

- Select the **Reflect** check box if you want to copy the ToS bytes of the inner IP packets to the outer IP packet headers.
- Enter the ToS byte value used by all packets sent across the pseudowire. The range is 0 to 255.

**Step 8** **Time To Live** Enter the value of the time to live (TTL) byte in the IP headers of tunneled packets. The range is 1 to 255.The default is 255.

**Step 9** **L2TP Class Name** Enter a unique L2TP class name if you want to configure multiple L2TP classes.

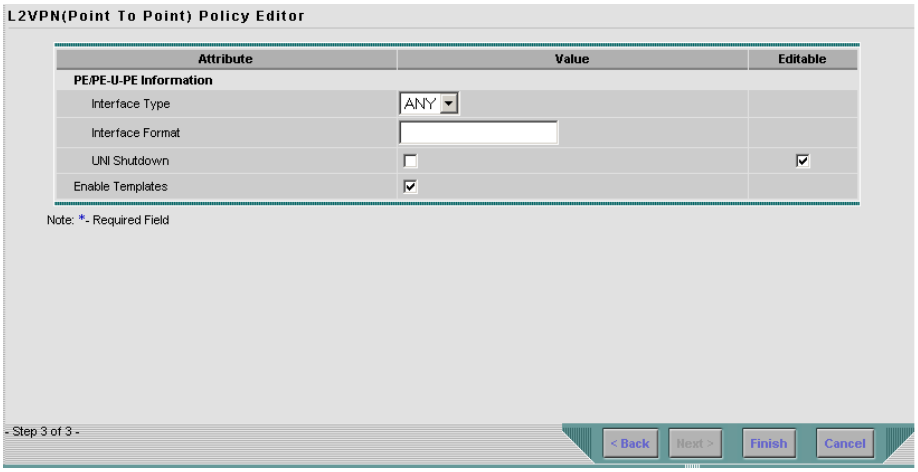
You must set up a tunnel name on two routers with same name. You can only have one tunnel per PE p air, but there can be many sessions in tunnel. For ATM, the vpi/vci pair for CE must match the vpi/vci pair for PE.

**Step 10** Select the **Transport Mode** from the drop-down list. The choices are:

- **VP** (Virtual Path)
- **VC** (Virtual Circuit) This is the default.

**Step 11** Click **Next**. The window in Figure 6-19 appears.

***Figure 6-19 ATM PE Policy Information***



**Step 12** Choose the PE **Interface Type** from the drop-down list. The choices are:

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

**Step 13** Enter the PE **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 14** Select the **UNI Shutdown** check box if you want to leave the UNI port shut during service activation, for example, when the service provider wants to deploy a service in the network but wants to activate it at a later time.

**Step 15** Select the **Enable Templates** check box if you want to download free-format CLIs to a device. If you enable templates, you can create templates and data files to push down to the router commands that are not normally supported by ISC. See *Cisco IP Solution Center Infrastructure Reference, 4.1* for more information about template management.

**Step 16** Click **Finish**.