Provision Circuits/VCs

Provision Circuits/VCs in Cisco EPN Manager

The process of creating and provisioning a circuit/VC is similar for all the supported technologies and involves:

- Specifying the endpoints of the circuit/VC.

- Defining the configuration parameters of the circuit/VC.

For a detailed overview of the provisioning support in Cisco EPN Manager, see Provision Circuits/VCs, on page 1.

To create and provision a new circuit/VC:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the circuit/VC.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**

Step 5 Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Note   You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**

Step 6   From the **Technology** drop-down list, choose the required technology. For example, if you are creating a circuit for Optical/DWDM network, choose **Optical**.

Step 7   In the **Service Type** area, choose the type of circuit/VC you want to create. For example, if you are creating a circuit/VC for Optical/DWDM network, the various circuit types include OCHNC WSON, OCHCC WSON, OCH-Trail WSON, OCH-Trail UNI, ODU UNI, ODU Tunnel and OPU over ODU.

Step 8   If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9   Click **Next** to go to the Customer Service Details page.

Step 10   (Optional) Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then go to the Provisioning Wizard to start provisioning the circuit/VC.

Step 11   Enter the service name and its description.

Step 12   From the **Deployment Action** drop-down list, choose the action that you want to perform after defining the attributes for the circuit/VC. The options are:

- **Preview**—Displays the generated CLIs for each device. You can review the CLIs and decide if you want to edit any attributes or go ahead with the deployment.

- **Deploy**—Deploys the configuration to the relevant devices immediately after you click **Submit** in the last page of the Provisioning Wizard.

Step 13   Click **Next** to choose the endpoints and define the attributes based on the technology you have selected.

Step 14   Click **Submit**. Depending on the deployment action you have chosen, the relevant action will be performed. That is, if you have chosen to preview the configuration, the preview page will be displayed where you can view the configurations, and then click **Deploy**. If you have chosen to deploy, the configurations will be directly deployed to the relevant devices.

Step 15   (Optional) Click the **Leave this View** button to continue using Cisco EPN Manager and to enable the service deployment to continue in the background.

> **Note**   If the device is busy, the request from Cisco EPN Manager to deploy the service will wait up to a pre-configured period of time before the request times out. To change this setting, see Set the Service Deployment Timeout Value, on page 3.

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the i icon next to the circuit/VC name to see the Circuit/VC 360 view.

For information about how to create and provision circuit/VCs for various technologies, see:

- Provision EVCs in a Carrier Ethernet Network, on page 6
- Provision Circuits in an Optical/DWDM Network, on page 16
- Provision L3VPN Services, on page 36
- Provision Circuit Emulation Services, on page 52
- Provision MPLS Traffic Engineering Services, on page 58

Set the Service Deployment Timeout Value

When you deploy a service to devices, if the devices are pre-occupied or busy, the service request created waits for a pre-configured period of time to acquire a 'device lock' for deploying the service. By default, the timeout value is set to 60 minutes.

To change the default timeout value:

Step 1   From the left sidebar, choose **Administration > Settings > System Settings**.

Step 2   Expand the **Circuits/VCs** section and click **Deployment Settings**.

Step 3   Set the required timeout value in minutes.

Cisco EPN Manager will now wait up to the specified time period to acquire the device lock for deploying the service. If the lock is not acquired within this time, the service deploy operation will fail.

What Happens When a Deployment Fails

When you deploy a circuit/VC, Cisco EPN Manager performs configuration changes in the participating devices based on the type of circuit/VC. Only when the configuration changes are successfully deployed to the devices, the circuit/VC will be considered as successfully provisioned. If the deployment of configuration changes fails in any one of the participating device, Cisco EPN Manager rolls back the configuration changes made so far in all the devices.

Deployment action can result in any one of the following scenarios:

- Deployment succeeds in all the participating devices; roll back is not initiated—In this scenario, all devices are successfully configured and the circuit provisioning is successful.

- Deployment fails; roll back is initiated and succeeds—In this scenario, when configuring multiple devices, the configuration fails in one of the device. The failure could be due to various reasons, for example, the device has declined the configuration. Cisco EPN Manager identifies the failure and successfully rolls back all the configuration changes that were made on all the devices. In this scenario, all device configurations are restored to the states, which were there before the deployment was attempted.

  Here is an example with three devices, A, B, and C, which are configured in a sequential order to provision a circuit. The configuration changes are deployed successfully in device A, but the deployment fails in device B. Cisco EPN Manager detects the failure and stops further configuration in devices B and C. It rolls back the configuration in the reverse order of provisioning, that is, it first rolls back the device B, followed by device A. Following are the actions that are performed sequentially in the three devices:

  - Device C—Rollback is not required for device C because there were no changes deployed to the device. This is because the configuration failure was detected in device B before configurations changes were sent to device C.

  - Device B—Cisco EPN Manager checks if there are any configuration changes made on this device before the deployment failed. If there are any changes, the partial configuration on this device is removed and the device is rolled back to the previous configuration.

  - Device A—Cisco EPN Manager performs a complete roll back in device A, where all the configuration changes that were successfully deployed earlier are removed and the device is rolled back to the previous configuration.

- Deployment fails; roll back is initiated but fails— In this scenario, when the configuration deployment fails on any of the participating device(s), Cisco EPN Manager performs a roll back, but the roll back on one or more devices fail. Now, the device(s) on which the roll back had failed, has the partial configuration.

  For example, the configuration changes are successfully deployed in devices A and B, the deployment fails in device C. Cisco EPN Manager identifies the failure and initiates the roll back in the reverse order of provisioning, that is, it first rolls back the device C, device B, and then device A. Following are the actions that are performed sequentially in the three devices:

  - Device C—Cisco EPN Manager performs a successful roll back in device C.

  - Device B—When attempting a rollback on device B, device connectivity is lost and there could be partial configurations left on the device.

  - Device A—Cisco EPN Manager performs a rollback of Device A, even if the roll back fails in device B.
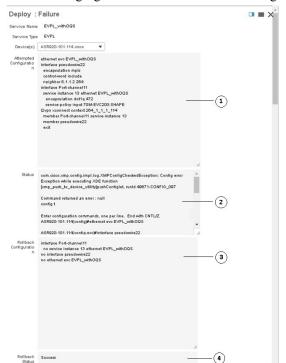
Note The roll back may fail due to various other reasons.

In the Provisioning Wizard, after previewing the configurations, click **Deploy**. When the deployment fails, the rollback configuration and the status for each participating device is displayed. From the **Device(s)** drop-down list, choose the device for which you want to view the rollback configuration and the status.

The following figure illustrates the rollback configuration and the rollback status for each device.

1	Attempted Configuration— Shows the configurations that were deployed to the device selected in the **Device(s)** drop-down list.
2	Deployment Status— Shows the deployment status of the selected device. If the deployment succeeds, it shows the status as "Success". If the deployment fails, it provides information about the failure.
3	Roll back Configuration— Shows the configurations for which rollback is automatically attempted.
4	Roll back Status— Shows the roll back status of the selected device. If the roll back succeeds, it shows the status as "Success". If the roll back fails, it provides information about the failure. You can use this information to manually clean up the partial configurations on the device.

You can also click the *i* icon next to the **Provisioning** column in the Circuits/VCs and Deleted Circuits/VCs tabs in the extended tables to view the details of configuration, configuration errors, rollback configuration, and rollback configuration errors for each device participating in the circuit/VC. The *i* icon is available for all provisioning states, except None. For information about how to access the extended tables, see View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map.

For information about how to troubleshoot deployment and rollback failures, see Troubleshoot Configuration Deployment Failures and Roll Back Failures, on page 5.

Troubleshoot Configuration Deployment Failures and Roll Back Failures

Following are the tips to troubleshoot the deployment or roll back failures:

- Deployment fails, but roll back succeeds— If the configuration deployment fails, roll back is automatically initiated and the results are displayed in the results page. Analyse the attempted configuration and error message shown in the results page for each device and identify the root cause of the deployment failure.

  The deployment failure could be due to, but not limited to the following issues:

    - Invalid values entered for the service parameters in the Provisioning Wizard. For example, the Service ID may already exists or there could be semantic errors in the CLI that is generated, and so on.

    - Device issues such as, device is not reachable, device password has changed, and so on.

  In this case, you must locate the circuit (by the name that you had given when creating it) for which deployment has failed, edit the circuit, and re-attempt the provisioning. If the service parameter for which the value to be changed is not editable, delete the circuit and create a new circuit.

  Note   Before deleting the circuit, ensure that it is not in use.

- Both, deployment and roll back fails— In this case, do the following:

  1. Ensure that the device is reachable and perform a device re-synch.

  2. If there were any device issues that were reported in the previous deployment, try to fix the issues.

  3. Edit the circuit and update the attributes, if required, and then re-attempt the circuit deployment.

  4. If the deployment fails, Cisco EPN Manager will initiate the roll back.

5. If the roll back fails again, identify the cause of the roll back failure.

6. To identify the cause of the failure, you can use the configuration and roll back transaction details, history of the service deployment attempts, and the roll back attempts that are displayed in the Circuit/VC 360 view. See Get Quick Information About a Circuit/VC: Circuit/VC 360 View.

7. Manually remove the partial configurations that are stored on the device.

You can also contact the Cisco representative to analyse and identify the root cause of configuration deployment failure and roll back failure.

Provision EVCs in a Carrier Ethernet Network

Summary of Cisco EPN Manager Carrier Ethernet Provisioning Support

This topic provides a summary of the Carrier Ethernet service provisioning support in Cisco EPN Manager 2.1. For a more detailed overview of the different types of EVCs and the supported underlying networks, see Overview of Circuit/VC Discovery and Provisioning.

Cisco EPN Manager supports provisioning of both port-based and VLAN-based VCs of the following types:

• E-line—Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL). See E-Line.
• E-LAN—EP-LAN and EVP-LAN. See E-LAN.
• E-Access—Access EPL and Access EVPL. See E-Access.
• E-TREE—EP-TREE and EVP-TREE. See E-Tree.

Cisco EPN Manager supports the following supplementary provisioning functions that can be used during EVC creation:

• Provision UNIs—For each EVC, you must define the attributes of the participating UNIs. You can either do this during the EVC creation or you can provision a UNI independently of the EVC creation process. See Configure a Device and Interface To Be a UNI, on page 15.
• Provision ENNI—For E-Access circuits, you must define the attributes of the ENNI. You can either do this during the EVC creation or you can provision an ENNI independently of the EVC creation process. See Configure a Device and Interface To Be an ENNI, on page 16.
• QoS Profiles—You can create QoS profiles to apply to VCs. See Create QoS Profiles, on page 78.
• EVC Attribute Profiles—You can create profiles containing all the required attributes for an EVC. These profiles can be selected during EVC creation to define the attributes of the EVC, instead of having to define the attributes individually for each EVC. See Create Circuit/VC Profiles , on page 77.

Prerequisites for EVC Provisioning

The following prerequisites must be met before you can provision EVCs:

1. Communication between devices must be set up before you can provision EVCs:

- In an MPLS end-to-end network, Label Distribution Protocol (LDP) must be set up across the network and each device must be provided with an LDP ID. This enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding. Alternatively MPLS end-to-end connectivity can be achieved using MPLS Traffic Engineering, and specifically, EVC provisioning over bidirectional TE tunnels is supported.
- If there is Ethernet access, i.e., not all devices are MPLS-enabled, G.8032 rings or ICCP-SM must be configured to connect the Ethernet access switch to the MPLS switch.
- CDP must be configured on the links within the G.8032 ring to enable Ethernet link discovery.

2. To provision EVCs over ICCP-SM and G.8032 networks, all VLANs (from 1 to 4095) should be configured either as primary or as secondary VLANs.

3. Inventory collection status for the devices on which the EVCs will be provisioned must be *Completed* . To check this, go to **Inventory > Network Devices**, and look at the status in the Last Inventory Collection Status column.

4. Customers can be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. Choose **Inventory > Other > Customers** in the left sidebar to create and manage customers.

5. For interfaces to be used in EVCs, it is recommended to reset the default configuration on the interfaces. In global configuration mode, configure the following command on each interface:

```
default interface 'interface-name'
```

6. For ME3600 and ME3800 devices, service instances can only be configured on trunk ports with no allowed VLANs. Configure the following commands on the interface and then re-sync the device in Cisco EPN Manager:

```
interface GigabitEthernetXX/XX
switchport trunk allowed vlan none
switchport mode trunk
```

Create and Provision a New Carrier Ethernet EVC

EVCs are created in the context of the topology map. You can access the topology map and the Provisioning Wizard by choosing **Configuration** > **Network** > **Service Provisioning** in the left sidebar or you can open the Provisioning Wizard from the topology map, as described in the procedure below.

The process of creating and provisioning an EVC is similar for all supported EVC types and involves:

- Specifying the endpoints (UNIs and ENNIs) of the EVC.
- Defining the configuration parameters of the circuit/VC.

Before you begin

For information about the prerequisites that must be met before you can provision EVCs, see .

To create a new EVC:

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the Device Groups button in the toolbar and select the group of devices you want to show on the map.

Step 3 In the Circuits/VCs tab, click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 4 Select **Carrier Ethernet** in the Technology drop-down list. Cisco EPN Manager displays a list of relevant circuit/VC types in the Service Type area. For example, Carrier Ethernet service types include EPL, EVPL, EP-LAN, and so on.

Step 5 In the Service Type list, select the type of circuit/VC you want to create.

Step 6 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 7 Click **Next** to go to the Service Details page.

Step 8 (Optional) Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 9 Enter the Service Details. See Service Details Reference, on page 11 for descriptions of the fields and attributes.

Step 10 For E-Line, E-Tree, and E-LAN EVCs: If required, configure the service OAM which enables fault and performance monitoring across the EVC. For E-Line EVCs, select the Enable CFM check box to enable the Service OAM options. You can then choose to either create a new CFM domain or select an existing domain for the E-Line EVC. See Service OAM, on page 14. Click the Plus icon to add a row to the Service OAM table and provide values in the relevant columns. For E-Tree EVCs, you must specify the direction, i.e., Leaf-to-Root, Root-to-Leaf, or Root-to-Root.

Step 11 In the Deployment Action field, specify what you want to do when the EVC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 12 Click **Next** to go to the page(s) in which you define the UNI(s). In the case of E-Access, there is an additional page for defining the ENNI.

Step 13 Identify the device and interface that will serve as the UNI:

> **Note** If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, select the Unmanaged check box and provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 80

- If you have already configured the required interface on the device as a UNI, uncheck the **Create New UNI** check box and select the relevant UNI Name from the list.

- To create a new UNI:

   - Make sure that the **Create New UNI** check box is checked.
   - In the UNI Name field, enter a name for the UNI that will enable easy identification of the UNI.
   - Select a device from the list in the Device field or click on a device in the map to select it and populate the Device field. A list of the selected device's ports is displayed.
   - Select the required port from the Port table. If the port cannot be used for the UNI, there is an alert icon next to the UNI name in the Port table that displays the reason why the port cannot be selected.

   > **Note** The device you select during UNI creation is circled in orange in the map. The UNI name is displayed above the orange circle. If it is a point-to-point EVC, the orange circle is labeled to indicate whether it is an A-side or Z-side endpoint.

Step 14 If you are creating a new UNI, enter the New UNI Details. See New UNI Details Reference, on page 12 for descriptions of the fields and attributes.

Step 15 Enter the UNI Service Details. See UNI Service Details Reference, on page 12 for descriptions of the fields and attributes.

Step 16 If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, select the **Unmanaged** check box and provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 80 for more information.

Step 17 For E-LAN and E-TREE EVCs with H-VPLS as the core technology, select the devices that will serve as the primary and secondary hubs.

Step 18   For E-Line and E-Access EVCs: In the Pseudowire Settings page, you can select a TE tunnel over which the EVC will traverse, as follows:

1. Check the **Static Preferred Path** check box to assign a static route for the service.

2. Choose the Preferred Path Type as Bidirectional or Unidirectional.

3. Select the required bidirectional TE tunnel from the Preferred Path drop-down list. This list contains all existing bidirectional TE tunnels between the endpoints of the EVC.

    Note   This field is available only if you selected **Bidirectional** as the Preferred Path Type.

4. Select the required unidirectional TE tunnels from the Preferred Path (A-Z) and Preferred Path (Z-A) drop-down lists.

    Note   These fields are available only if you selected **Unidirectional** as the Preferred Path Type.

5. Select the **Allow Fallback to LDP** check box if you want the default path to be used if the preferred path is unavailable.

    Note   If no tunnel exists between the endpoints, the Preferred Path and the Fallback to LDP options will be disabled.

6. Select the **Send Control Word** check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.

7. Select the **Interworking Option** if you need to interconnect sites using either Ethernet, VLAN, or IP. This option must be enabled if one of the endpoints in the EVC is an unmanaged device.

8. Enter the required bandwidth for the pseudowire.

Step 19   (Optional) If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the Service Template page. See Extend a Circuit/VC Using Templates, on page 80 for more information.

Step 20   When you have provided all the required information for the circuit/VC, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

Step 21   The circuit/VC should be added to the list in the Circuits/VCs tab in the Network Topology window.

If the configuration deployment fails, see the What Happens When a Deployment Fails, on page 3 section.

Create and Provision an EVC with Multiple UNIs

Cisco EPN Manager supports creating/selecting multiple UNIs during the creation and provisioning of multipoint EVCs (E-LAN and E-Tree).

Note   You can have multiple UNIs on the same device for EVCs using VPLS as the core technology, but not for H-VPLS-based EVCs.

Before you begin

For information about the prerequisites that must be met before you can provision EVCs, see Prerequisites for EVC Provisioning, on page 6.

To create a new EVC:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

Step 3 Click the **Circuits/VCs** tab.

Step 4 From the **Circuits/VCs** pane toolbar, click the + (**Create**) icon.

The Provisioning Wizard opens in a new pane to the right of the map.

Step 5 Select **Carrier Ethernet** in the Technology drop-down list

Step 6 In the Service Type list, select a multipoint EVC type.

Step 7 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 8 Click **Next** to go to the Service Details page.

Step 9 Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 10 Enter the Service Details. See Service Details Reference, on page 11 for descriptions of the fields and attributes.

Step 11 In the Deployment Action field, specify what you want to do when the EVC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 12 Click Next to go to the page(s) in which you define the UNI(s).

Step 13 In the Multi UNI area, click the Plus icon to add the first UNI to the table. The UNI is given a default name and is automatically selected in the table. Each time you click the Plus icon, a new UNI is added to the table.

Alternatively, you can click on devices in the map to add new UNIs to the table. In this case, the device name will be populated in the Device field under New UNI details.

Step 14 Select a UNI in the table to define or edit its attributes.

Step 15 Identify the device and interface that will serve as the UNI:

- To use an existing UNI, uncheck the Create New UNI check box and select the relevant UNI Name from the list.
- To define a new UNI:

  - Make sure that the Create New UNI check box is checked.
  - In the UNI Name field, enter a name for the UNI that will enable easy identification of the UNI.
  - Select a device from the list in the Device field. A list of the selected device's ports is displayed.
  - Select the required port from the Port table. If the port cannot be used for the UNI, there is an alert icon next to the UNI name in the Port table that displays the reason why the port cannot be selected.

Step 16 If you are creating a new UNI, enter the New UNI Details. The New UNI details are relevant for the UNI that is currently selected in the Multi UNI table. See New UNI Details Reference, on page 12 for descriptions of the fields and attributes.

Step 17 Enter the UNI Service Details. See UNI Service Details Reference, on page 12 for descriptions of the fields and attributes. Click Next.

Step 18 If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, provide information for the unmanaged device in the Unmanaged page. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 80

Step 19 Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the Service Template page. See Extend a Circuit/VC Using Templates for more information.

Step 20 When you have provided all the required information for the circuit/VC, click Submit. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

Step 21 The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window.

Service Details Reference

The following table lists and describes the attributes that define the EVC on the service level. Note that not all attributes are relevant for all the EVC types.

Table 1: Service Details

Attribute	Description
Service Name	Unique name to identify the circuit/VC.
Service Description	Description of the VC that will help to identify the VC.
Service Type	Prepopulated based on the type of service you are creating—EPL, EVPL, EP-LAN, and so on.
Service MTU	The maximum size, in bytes, of any frame passing through the VC. Values can be between 1522 and 9216. The service MTU must be lower than or equal to the MTU defined on all of the service's UNIs.
Core Technology	VPLS or H-VPLS. See Core Technology for Multipoint EVCs.
VPN ID	Relevant for multipoint EVCs (both VPLS and H-VPLS). This field is automatically populated with the next available pseudowire ID. This ID can be changed during the EVC creation process (valid value range: 1-4294967295). The ID is not editable when modifying the EVC. **Note** The VPN ID is used uniquely across the network, meaning that two services will not use the same VPN ID. In addition, the VPN ID cannot use a pseudowire ID which is already configured in the network to avoid pseudowire ID collision.
Bundling	Enables multiple VLANs on this VC. Multiple CE-VLAN IDs are bundled to one EVC.
CE-VLAN ID Preservation	Ensures that the CE-VLAN ID of an egress service frame is identical in value to the CE-VLAN ID of the corresponding ingress service frame. This must be enabled if bundling is enabled.
CE-VLAN ID CoS Preservation	Ensures that the CE-VLAN CoS of an egress service frame is identical in value to the CE-VLAN CoS of the corresponding ingress service frame. The CoS markings are unaltered.

New UNI Details Reference

The following table lists and describes the attributes relating to the port that is specified as the UNI. Note that not all attributes are relevant for all the EVC types.

Table 2: New UNI Details

Attribute	Description
MTU	The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the UNI must be greater than or equal to the MTU defined on the service level.
Speed	Port speed. You can reduce the speed if this is supported on the port.
Duplex Mode	• Full Duplex—Uses simultaneous communication in both directions between the UNI and the customer's access switch, assuming that both sides support full duplex. If one side does not support full duplex, the port will be brought down. • Auto-Negotiation—Uses the mode that is agreed upon between the two devices, depending on what is supported. Full Duplex will be attempted but if one device does not support it, half duplex will be used.
Service Multiplexing	Allows the UNI to participate in more than one EVC instance.
UNI Allows Bundling	Allows the UNI to participate in VCs with Bundling enabled. See Bundling in Service Details Reference, on page 11
Untagged CE-VLAN ID	The ID of the CE-VLAN assigned to untagged traffic.
Ingress/Egress QoS Profile	Select the required QoS profile for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to Create QoS Profiles, on page 78 for information on how to create QoS profiles.
UNI QoS Profile	Applies a QoS profile on the UNI itself to define the bandwidth profile and other quality of service attributes of the UNI. If you apply a QoS profile on the UNI level, you should not apply a QoS profile on the service level.
Enable Link OAM	Enables IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch.
Enable Link Management	Enables the customer access switch to get information about this UNI, VLAN IDs, services on the UNI, and so on.

UNI Service Details Reference

The following table lists and describes the attributes of the EVC in relation to the UNI, i.e., how the EVC operates on this UNI. Note that not all attributes are relevant for all the EVC types.

> **Note** For QinQ attributes, only the attributes that are supported on the selected device will appear in the wizard.

Table 3: UNI Service Details

Attribute	Description	Additional Information
Ingress/Egress Service QoS Profile	Select the required QoS profile for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to Create QoS Profiles, on page 78 for information on how to create QoS profiles.	
Layer 2 Control Protocol Profile	Profile that determines how the various communication protocols are handled. Frames using the various protocols are either tunneled, dropped or peered. Refer to MEF 6.1 for details.	
Designation	For E-Tree: Select the role of the UNI in the VC, either Leaf or Root.	
Use point to point connection with Root	For E-Tree: If the UNI is designated as a leaf, you can select this check box to create an active pseudowire between root and leaf. The check box will not appear if there is more than one endpoint on a single device or if there is more than one root in the service.	
Match	Select the type of tagging the traffic should have in order to enter the UNI: • Dot1q—Mapping of 802.1q frames ingress on an interface to the service instance. • Dot1ad—Mapping of 802.1ad frames ingress on an interface to the service instance. • Default—Traffic that is not assigned to any other VC on this port. • Untagged—Frames that have no VLAN tag	Dot1AD is not supported on ME3600 devices running15.3(3)software version.
Auto Allocate VLAN	Check this check box to automatically allocate a VLAN ID for the UNI.	
VLAN(s)	VLAN identifier, an integer between 1 and 4094. You can enter a range of VLAN IDs using a hyphen or a comma-separated series of VLAN IDs.	This field is not available if you have checked the Auto Allocate VLAN check box.
Inner VLAN(s)	VLAN identifier for the second level of VLAN tagging, an integer between 1 and 4094. You can enter a range of VLAN IDs using a hyphen or a comma-separated series of VLAN IDs.	
Untagged Bundled	Enables traffic with no VLAN tags to be bundled together with VLAN tagged frames.	
Priority Tagged Bundled	Enables priority tagged traffic to be bundled together with VLAN tagged frames.	
Exact	Prevents admittance of traffic with additional inner VLAN tags other than those that are matched to be carried by the service.	Applicable for IOS-XR devices only.
Outer VLAN CoS	The outer VLAN Class of Service identifier that should be associated with the frame. The CoS ID can be an integer between 0 and 7.	Applicable for IOS devices only.

Attribute	Description	Additional Information
Inner VLAN CoS	The inner VLAN Class of Service identifier that should be associated with the frame. The CoS ID can be an integer between 0 and 7.	Applicable for IOS devices only.
E-Type	Limits the service to only carry frames of the specified Ethertype: • IPv4 • IPv6 • PPPoE-All • PPPoE-Discovery • PPPoE-Session	Applicable for IOS devices only.
Rewrite Definition Action	The encapsulation adjustment to be performed when the frame enters the UNI: • None • Pop—Removes one or two VLAN tags from the frame on ingress and adds them on egress. • Push—Adds one or two VLAN tags from the frame on ingress and removes them on egress., either Dot1q or Dot1ad tags. • Translate—Replaces VLAN tags with new VLAN tags, either Dot1q or Dot1ad tags The translation can be 1:1, 1:2, 2:1, or 2:2.	The Translate action is applicable for IOS-XR devices only.

Service OAM

On the service level, you can define EOAM (Ethernet Operations, Administration and Management) parameters that will allow monitoring and troubleshooting of the EVC. Effectively, you will be configuring Connectivity Fault Management (CFM) components on the endpoints of the EVC.

For a point-to-point EVC, you can define OAM parameters in one direction, i.e., from UNI A to UNI Z or in both directions. For a multipoint EVC, you can define the source and destination MEP groups and then associate the EVC endpoints with a specific MEP group.

See Configure EOAM Fault and Performance Monitoring for more information about CFM and for device-level CFM configuration.

Use the Service OAM section in the Customer Service Details page of the Provisioning Wizard to define the specifications of the service frame to be monitored and to define the OAM profile to apply to that frame, as follows:

- From—The source of the traffic flow across the EVC.
- To—The destination of the traffic flow across the EVC.
- Direction (E-Tree only) —The direction of traffic flow between leaf and root, or root to root.

Note Your input in the From and To fields creates MEP groups, or ordered sets of UNIs. In the next page of the wizard, you will associate the UNI with one of these MEP groups.

- CoS—The Class of Service identifier that should be associated with the frame.
- OAM Profile—A set of OAM attributes that should be applied to the frame to enable performance monitoring. The following OAM profiles are available for selection:

- Performance Monitoring 1: Enables continuity check and synthetic loss measurement.
- Performance Monitoring 2: Enables continuity check, synthetic loss measurement, and single-ended delay measurement.
- Performance Monitoring 3: Enables continuity check, synthetic loss measurement, and dual-ended delay measurement.

- Continuity Check Interval—The interval between continuity check messages.

Configure a Device and Interface To Be a UNI

The User Network Interface (UNI) is the physical demarcation point between the responsibility of the Subscriber (the Customer Edge or CE) and the responsibility of the Service Provider (the Provider Edge or PE).

UNIs demarcate the endpoints of EVCs, so configuring device interfaces as UNIs is an essential part of VC provisioning. UNI configuration can be done during the VC creation process. Alternatively, you can configure UNIs independently of VC creation. These UNIs will be available for selection during VC creation.

To configure a UNI:

Step 1 Follow the instructions in Create and Provision a New Carrier Ethernet EVC, on page 7 to access the Provisioning Wizard.

Step 2 Select **Carrier Ethernet** from the Technology drop-down list.

Step 3 Select **UNI** from the Service Types list.

Step 4 Click **Next** to go to the Customer Service Details page.

Step 5 Provide a unique name and description for the UNI, and associate it with a customer, if required.

Step 6 Define the service attributes of the UNI, as follows:

- All to One Bundling—For port-based VCs where the UNI is dedicated to the VC. When enabled, all CE-VLAN IDs are bundled to one VC. When All to One Bundling is selected, Multiplexing and Bundling cannot be selected.

- Service Multiplexing—For VLAN-based VCS where the UNI is shared between multiple VCs. When enabled, allows the UNI to participate in more than one EVC instance.

- Bundling—Allows the use of multiple VLANs for this UNI. Multiple CE-VLAN IDs are bundled to one EVC.

Step 7 Under Deploy, select whether you want to deploy the UNI immediately upon completion or first display a preview of the CLI that will be deployed to the device.

Step 8 Click **Next** to go to the UNI Details definition page.

Step 9 Select the device and port you want to configure as the UNI.

Step 10 Configure the UNI attributes, as described in New UNI Details Reference, on page 12.

Step 11 Click **Submit**. If you previously chose to deploy the circuit upon completion, a job is created and the required CLI is deployed to the devices. If you chose to see a preview of the CLI before actually deploying to the devices, the preview will be displayed now . Verify the CLI and if you want to change any of the attributes, click **Edit Attributes**. Else, click **Deploy**.

Configure a Device and Interface To Be an ENNI

The External Network to Network Interface (ENNI) specifies the reference point that is the interface between two Metro Ethernet Networks (MENs) where each operator network is under the control of a distinct administration authority. The ENNI is intended to support the extension of Ethernet services across multiple operator MENs, while preserving the characteristics of the service.

When provisioning an E-Access VC, you need to define the ENNI that will carry traffic through to the adjacent network. ENNI configuration can be done during the VC creation process. Alternatively, you can configure ENNIs independently of VC creation. These ENNIs will be available for selection during VC creation.

To configure an ENNI:

Step 1 Follow the instructions in to access the Provisioning Wizard.

Step 2 Select **Carrier Ethernet** from the Technology drop-down list.

Step 3 Select **ENNI** from the Service Types list.

Step 4 Click **Next** to go to the Customer Service Details page.

Step 5 Provide a unique name and description for the ENNI, and associate it with a customer/operator, if required.

Step 6 Under Deploy, select whether you want to deploy the ENNI immediately upon completion or first display a preview of the CLI that will be deployed to the device.

Step 7 Click **Next** to go to the ENNI Details definition page.

Step 8 Select the device and port(s) you want to configure as the ENNI.

Step 9 Define the following parameters for the ENNI:

- MTU—The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the ENNI must be greater than 1526.

- Speed—If required, you can reduce the speed of the port if this is supported.

- Protection Mechanism—This defines the resiliency scheme at the ENNI. If you have selected more than one port for this ENNI, you can specify whether to apply a protection mechanism, which could be Link Aggregation or another agreed upon protection mechanism. Selecting Link Aggregation creates a Link Aggregation Group (LAG) with two links. If one of the links fails, traffic is moved to the other link.

Step 10 Click **Submit**. If you previously chose to deploy the circuit upon completion, a job is created and the required CLI is deployed to the devices. If you chose to see a preview of the CLI before actually deploying to the devices, the preview will be displayed now. Verify the CLI and if you want to change any of the attributes, click **Edit Attributes**. Else, click **Deploy**.

Provision Circuits in an Optical/DWDM Network

Summary of Cisco EPN Manager Optical/DWDM Network Provisioning Support

Cisco EPN Manager supports the provisioning of Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit types. The DWDM optical technology is used to increase bandwidth over existing fiber optic backbones. It combines and transmits multiple signals simultaneously at different wavelengths on the same fiber. In effect, one fiber is transformed into multiple virtual fibers.

Cisco EPN Manager supports the following optical circuits:

- Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit—Following are the different optical channel circuit types:
    - Optical Channel Network Connection (OCHNC) WSON—OCHNC WSON circuits establish connectivity between two optical nodes on a specified C-band wavelength. For more information, see Optical Channel Network Connection (OCHNC) WSON.
    - Optical Channel Client Connection (OCHCC) WSON—OCHCC WSON circuits extend the OCHNC WSON to create an optical connection from the source client port to the destination client port of the TXP/MXP cards. For more information, see Optical Channel Client Connection (OCHCC) WSON.
    - Optical Channel (OCH) Trail WSON— OCH trail WSON circuits transport the OCHCC WSON circuits. For more information, see Optical Channel (OCH) Trail WSON.
    - Optical Channel (OCH) Trail connecting NCS 1002, NCS 55xx, and ASR 9K devices—This OCH trail circuit creates an optical connection from the source trunk port of an NCS 1002, NCS 55xx, or ASR 9K device to the destination trunk port of another similar device. For more information, see Optical Channel (OCH) Trail Connecting NCS 1002, NCS 55xx, and ASR 9K Devices
    - Optical Channel (OCH) Trail User-to-Network Interface (UNI)—An OCH trail UNI circuit establishes connectivity between Cisco NCS 2000 series devices and Cisco NCS 4000 series devices. For more information, see Optical Channel (OCH) Trail User-to-Network Interface (UNI).
    - Spectrum Switched Optical Network (SSON)—SSON circuits allow you to provide more channels in a span. Using the SSON functionality, the circuits are placed closer to each other if they are created within a media channel group. For more information, see Spectrum Switched Optical Network (SSON) Circuits.

- Optical Transport Network (OTN)—An OTN circuit can be established statically or dynamically between ingress and egress nodes using Resource Reservation Protocol (RSVP) signaling. For more information, see Optical Transport Network (OTN) Circuit.
    - Optical Channel Data Unit User-to-Network Interface (ODU UNI)—An ODU UNI circuit represents the actual end-to-end client service passing through the OTN architecture. For more information, see Optical Channel Data Unit User-to-Network Interface (ODU UNI).
    - Optical Channel Data Unit (ODU) Tunnel—ODU tunnel circuits transport the ODU UNIs. For more information, see Optical Channel Data Unit (ODU) Tunnel.
    - Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU)—OPU over ODU circuits provide a high-bandwidth point-to-point connection between two customer designated premises.These circuits uses ODU UNI circuits to carry client signals through the network. For more information, see Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU).

- Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin—An ODU UNI Hairpin circuit is similar to an ODU UNI circuit, but it is created in the management plane and it is an intra node circuit, that is, the source and destination is the same device but with different interfaces. For more information, see Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin.

- Optical Channel Data Unit (ODU)—Optical Channel Data Unit (ODU) is created as a sub controller of an OTU controller. ODU contains information for the maintenance and operational functions to support optical channels. For more information, see Optical Channel Data Unit (ODU).

Prerequisites for Provisioning Optical Circuits

Following are the prerequisites for provisioning an optical circuit:

- Cisco EPN Manager supports both, Wavelength Switched Optical Network (WSON) and non-WSON circuits. However, for non-WSON circuits, Cisco EPN Manager supports only circuit discovery, which includes circuit overlay, circuit 360 view, multilayer trace view, and circuit details. Cisco EPN Manager does not support the provisioning, activation, deactivation, protection switch actions, and modification of non-WSON circuits.
- Communication between devices must be set up before you can provision an optical circuit.
- Inventory collection status for the devices on which the optical circuits will be provisioned must be Completed. To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the Last Inventory Collection Status column.
- DWDM grid unit must be set to either, wavelength or frequency. To do this, go to **Administration** > **Settings** > **System Settings** > **Circuits/VCs Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.
- Before you provision an OCHNC or a Media Channel NC circuit using NCS 2000 series devices running on software version 10.7 or later, ensure that you create a UNI config, either in Cisco Transport Controller (CTC) or in Cisco EPN Manager.

- Optionally, customers must be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.

Create and Provision an OCH Circuit

To provision an OCH circuit:

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 18.

Step 1   From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2   Click **Device Groups**, and then select the location in which you want to create the OCH circuit.

Step 3   Close the **Device Groups** popup window.

Step 4   In the **Network Topology** window, click **Circuits/VCs**.

Step 5   Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, Optical service types for OCH circuits include OCHNC WSON, OCHCC WSON, OCH-Trail WSON, and OCH-Trail UNI.

Step 7 In the **Service Type** area, choose the type of OCH circuit you want to create.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11 Enter the circuit name and its description in the **Customer Section** page.

Step 12 Click **Next** to go to the **Circuit Section** page.

> **Note** If you select OCH-Trail UNI as the optical service type, the **Endpoint Section** page appears first followed by the **Circuit Section** page.

Step 13 Enter the circuit details. See Circuit Section Reference for OCH Circuit Types, on page 19 for descriptions of the fields and attributes.

Step 14 Click **Next** to go to the **Endpoint Section** page.

Step 15 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name, Termination Point, and Add/Drop Port columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.

> **Note** When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column and select the endpoints for the available cards.

> **Note** The **Add Port** and **Drop Port** columns is available only for OCHNC WSON circuit. Once you choose the port that needs to be added to the Add Port column, the value in the Drop Port column gets auto-populated. Also, you can manually edit the values in the Drop Port column.

Step 16 Click **Next** to go to the **Constraints Section** page.

Step 17 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

> **Note** When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

Step 18 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it but you cannot edit the attributes.

Step 19 The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Circuit Section Reference for OCH Circuit Types

The following table lists and describes the attributes that define the OCH circuit types.

Table 4: Circuit Section Reference—OCH Circuit Types

Attribute	Description	Enabled
Circuit Details		
Label	Unique name to identify the circuit.	
State	Administrative state for the circuit. Values are: • In Service—The circuit is in service and able to carry traffic. • Out of Service—The circuit is out of service and unable to carry traffic.	For all OCH circuit types.
Bi-directional	Check this check box to create a two-way circuit.	For OCHCC WSON and OCH Trail WSON circuit types.
Protection	Protection mechanism for the circuit. Cisco EPN Manager supports the following protection mechanism based on the circuit type selected: • None—For unprotected circuits. This value is available for all OCH circuit types.. • PSM—When a Protection Switch Module (PSM) card is connected to a TXP card. This value is available for OCHNC WSON and OCHCC WSON circuit types. • Y-Cable—When a transponder or muxponder card protects the circuit. This value is available for OCHCC WSON circuit type. • Splitter—When a MXPP/TXPP card is used. The circuit source and destination are on MXPP_MR_2.5G and TXPP_MR_2.5G cards. These cards provides splitter (line-level) protection (trunk protection typically on TXPP or MXPP transponder cards). This value is available only for OCHCC WSON circuit type.	For OCHNC WSON circuit type.
Route Properties		
Diverse From Tunnel	Select a tunnel to ensure that it is not used by the circuit you are provisioning. This is to ensure that if there is a failure in a tunnel, the same tunnel is not used by another circuit.	For OCH-Trail UNI circuit types when the Mutual Diversity check box is unchecked.
Validation	Validation mode for the circuit. Values are: • Full—The circuit is created when the circuit validation result is greater than or equal to the acceptance threshold value. • None—The circuit is created without considering the acceptance threshold value.	For all OCH circuit types.

Attribute	Description	Enabled
Acceptance Threshold	Protection acceptance threshold value set for the OCH protected circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all OCH circuit types when the Validation field is set to Full.
Protect Acceptance Threshold	Protection acceptance threshold value set for the OCH protected circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For OCHNC WSON circuit type when: • Protection field is set to PSM, Y-Cable, or Splitter.. • Validation field is set to Full.
Ignore Path Alarms	Check the check box to ignore path alarms.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types.
Allow Regeneration	Check the check box to allow the network elements to regenerate the signal.	For all OCH circuit types.
Restoration	Check this check box to restore the failed OCH circuit to a new route.	For all OCH circuit types.
Priority	Prioritize the restoration operation for the failed OCH circuit. Values are High, Priority 1, Priority 2, Priority 3, Priority 4, Priority 5, Priority 6, and Low.	For all OCH circuit types when the Restoration check box is checked.
Restoration Validation	Validation mode for the restoration operation. Values are: • None—The circuit is restored without considering the restoration acceptance threshold value. • Inherited— The restoration circuit inherits the validation and acceptance threshold values from the primary circuit. • Full—The circuit is restored when the restoration validation result is greater than or equal to the restoration acceptance threshold value.	For all OCH circuit types when the Restoration check box is checked.

Attribute	Description	Enabled
Restoration Acceptance Threshold	Acceptance threshold value set for the restoration operation for OCH circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all OCH circuit types when: • Restoration check box is checked. • Restoration Validation field is set to Full.
Restoration Protect Acceptance Threshold	Protection acceptance threshold value set for the restoration operation for OCH protected circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For OCHNC WSON circuit type when: • Protection field is set to PSM, Y-Cable, or Splitter.. • Restoration check box is checked. • Restoration Validation field is set to Full.
Revert	Reverts the circuit from the restored path to the original path after a failure is fixed. Values are None, Manual, and Automatic.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when the Restoration check box is checked.
Soak Time	Period that the circuit on the restored path waits before switching to the original path after a failure is fixed.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when Revert is set to Manual or Automatic.
Admin State	Select the admin state of the circuit as **Up** or **Down**. This impacts the circuit's operability and determines whether the circuit can be activated or deactivated.	For OCH-Trail UNI circuit type.
Preferred Wavelength Properties		
Wavelength Options	Wavelength options for the circuit. Values are **Do Not Set**, **Set To Default**, and **Set Preferred Wavelength**.	For OCH-Trail UNI circuit type.
Work Port Properties		
Auto Provisioning	Check this check box to enable the Auto Provisioning feature.	For all OCH circuit types

Attribute	Description	Enabled
C Band	Conventional wavelength window to provision the circuit. Values are: • Odd—The odd position in the ITU grid. • Even—The even position in the ITU grid.	• For all OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when the Auto Provisioning check box is unchecked. • For OCH-Trail UNI circuit type when the Wavelength Options is set to Set Preferred Wavelength.
Wavelength/Frequency	Wavelength or frequency of the circuit. This value is applicable for the C Band that you chose. **Note** You must set the DWDM grid unit to either wavelength or frequency. To do this, go to **Administration** > **Settings** > **System Settings** > **Circuits/VCs Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.	For all OCH circuit types when the C Band field is set to Odd or Even.
Preferred/Required	Select to determine whether the values set in the C Band and Wavelength/Frequency fields are preferred or required to provision the circuit.	For all OCH circuit types when the Auto Provisioning check box is unchecked.
Protect Port Properties		
Copy from Work Port	Check this check box to copy the values set in the Work Port Properties section.	For all OCH circuit types when the Protection field is set to PSM, Y-Cable, or Splitter.

Create and Provision Two Mutually Diverse OCH-Trail UNI Circuits

Use this procedure to create two OCH-Trail UNI circuits that are mutually diverse from each other. Both the circuits must originate from the same device. You can create both the circuits quickly using the Provisioning wizard in a single workflow .

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 18.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the OCH circuit.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**.

Step 7 In the **Service Type** area, choose **OCH-Trail UNI**.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 Check the **Mutual Diversity** check box to create two OCH-Trail UNI circuits that are mutually diverse from each other.

Step 11 Enter the circuit name and its description in the **Customer Section** page.

Step 12 Click **Next** to go to the **Endpoint Section** page.

Step 13 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Interface.

> **Note** When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.

Step 14 Click **Next** to go to the **Circuit Section** page.

Step 15 Enter the circuit details. See Circuit Section Reference for OCH Circuit Types, on page 19 for descriptions of the fields and attributes.

Step 16 Click **Next** to go to the **Constraints Section** page.

Step 17 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

> **Note** When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

Step 18 Click **Next**. The **Customer Section** page for the second circuit is displayed.

Step 19 Repeat Step 11 to Step 17 to create the second circuit.

Step 20 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it but you cannot edit the attributes.

Step 21 The circuits should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC names to see the Circuit/VC 360 view.

Create and Provision a Media Channel Group SSON Circuit

To create and provision a Media Channel Group SSON circuit:

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 18.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the Media Channel Group SSON circuit.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area.

Step 7 In the **Service Type** area, choose **Media Channel Group SSON**.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11 Enter the circuit name and its description in the **Customer Section** page.

Step 12 Click **Next** to go to the **Endpoint Section** page.

Step 13 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name, Termination Point, and Add/Drop Port columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.

> **Note** When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.

Step 14 Click **Next** to go to the **Circuit Section** page.

Step 15 Choose the required circuit width.

Step 16 To set the **Central Wavelength/Frequency Properties**, do one of the following:

- Check the **Auto Provisioning** check box.
- Choose the required **Wavelength** for the circuit and then choose either **Preferred** or **Required** option to determine whether the values set in the **Wavelength** field is preferred or required to provision the circuit.

Step 17 Click **Next** to go to the **Constraints Section** page.

Step 18 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

Note	When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

Step 19   Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Create and Provision a Media Channel SSON Circuit

To create and provision a Media Channel SSON circuit:

Before you begin

- Ensure that a Media channel group SSON is already created to associate the Media Channel SSON circuits with the Media channel group. See Create and Provision a Media Channel Group SSON Circuit, on page 25.

- For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 18.

Step 1   From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2   Click **Device Groups**, and then select the location in which you want to create the Media Channel SSON circuit.

Step 3   Close the **Device Groups** popup window.

Step 4   In the **Network Topology** window, click **Circuits/VCs**.

Step 5   Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6   From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, optical service types for Media Channel SSON circuits include Media Channel NC SSON, Media Channel Trail SSON, and Media Channel CC SSON.

Step 7   In the **Service Type** area, choose the type of Media Channel SSON circuit you want to create.

Step 8   If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9   Click **Next** to go to the **Customer Section** page.

Step 10   (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11   Enter the circuit name and its description in the **Customer Section** page.

Step 12   Click **Next** to go to the **Endpoint Section** page.

Step 13   Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Termination Point columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.

Note	The MCH-Trail Name column is available only when you create a Media Channel CC SSON circuit.

Step 14 Click **Next** to go to the **Circuit Section** page.

Note	For the Media Channel CC SSON circuits, the **Circuit Section** page is not available if you have entered an MCH-Trail Name in the Endpoints table.

Step 15 Choose the Media Channel Group to which you want to associate the Media Channel SSON circuit.

Step 16 Enter the circuit details. See Circuit Section Reference for Media Channel SSON Circuit Types, on page 27 for descriptions of the fields and attributes.

Step 17 Click **Next** to go to the **Constraints Section** page.

Step 18 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

Note	When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

Step 19 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Circuit Section Reference for Media Channel SSON Circuit Types

The following table lists and describes the attributes that define the Media Channel SSON circuit types.

Table 5: Circuit Section Reference—Media Channel SSON Circuit Types

Attribute	Description	Enabled
Central Wavelength/Frequency Properties		
Auto Provisioning	Check this check box to automatically set the wavelength or frequency properties for the circuit.	For all Media Channel SSON circuit types.
Wavelength (nm)	Wavelength or frequency of the circuit. **Note** You must set the DWDM grid unit to either wavelength or frequency. To do this, go to **Administration** > **Settings** > **System Settings** > **Circuits/VCs Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.	For all Media Channel SSON circuit types when the Auto Provisioning check box is unchecked.
Preferred/Required	Select to determine whether the values set in the Wavelength field is preferred or required to provision the circuit.	For all Media Channel SSON circuit types when the Auto Provisioning check box is unchecked.

Attribute	Description	Enabled
Optical Properties		
Validation	Validation mode for the circuit. Values are: • Full—The circuit is created when the circuit validation result is greater than or equal to the acceptance threshold value. • None—The circuit is created without considering the acceptance threshold value.	For all Media Channel SSON circuit types.
Acceptance Threshold	Protection acceptance threshold value set for the circuit. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all Media Channel SSON circuit types when the Validation field is set to Full.
Ignore Path Alarms	Check the check box to ignore path alarms.	For all Media Channel SSON circuit types.
Allow Regeneration	Check the check box to allow the network elements to regenerate the signal.	For all Media Channel SSON circuit types.
Restoration	Check this check box to restore the failed Media Channel SSON circuit to a new route.	For all Media Channel SSON circuit types.
Priority	Prioritize the restoration operation for the failed circuit. Values are High, Priority 1, Priority 2, Priority 3, Priority 4, Priority 5, Priority 6, and Low.	For all Media Channel SSON circuit types when the Restoration check box is checked.
Restoration Validation	Validation mode for the restoration operation. Values are: • None—The circuit is restored without considering the restoration acceptance threshold value. • Inherited— The restored circuit inherits the validation and acceptance threshold values from the primary circuit. • Full—The circuit is restored when the restoration validation result is greater than or equal to the restoration acceptance threshold value.	For all Media Channel SSON circuit types when the Restoration check box is checked.

Attribute	Description	Enabled
Restoration Acceptance Threshold	Acceptance threshold value set for the restoration operation for the circuit. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all Media Channel SSON circuit types when: • Restoration check box is checked. • Restoration Validation field is set to Full.
Revert	Reverts the circuit from the restored path to the original path after a failure is fixed. Values are None, Manual, and Automatic.	For all Media Channel SSON circuit types when the Restoration check box is checked.
Soak Time	Period that the circuit on the restored path waits before switching to the original path after a failure is fixed.	For all Media Channel SSON circuit types when the Revert option is set to Manual or Automatic.

Create and Provision an OTN Circuit

To provision an OTN circuit:

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 18.

Step 1   From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2   Click **Device Groups**, and then select the location in which you want to create the OTN circuit.

Step 3   In the **Network Topology** window, click **Circuits/VCs**.

Step 4   Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 5   From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, service types for OTN circuits include ODU UNI, ODU Tunnel, OPU over ODU, and ODU UNI Hairpin.

Step 6   In the **Service Type** area, choose the type of OTN circuit you want to create.

Step 7   If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 8   Click **Next** to go to the **Customer Details** page.

Step 9   (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 10   Enter the circuit name and its description in the **Customer Details** page.

Step 11   Click **Next** to go to the **Circuit Details** page.

Step 12   Enter the circuit details. See Circuit Section Reference for OTN Circuit Types, on page 30 for descriptions of the fields and attributes.

Step 13   Click **Next** to go to the **Endpoint Section** page.

Step 14   Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Interface/Termination Point columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.

> **Note**   When the row is in the edit mode, you cannot click a device in the map to populate the Device Name column.

Step 15   Enter the protection type and path options for the circuit. See Endpoint Section Reference for OTN Circuit Types, on page 31 for descriptions of the fields and attributes.

Step 16   Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview**. After seeing the preview of the TL1 or CLI commands, you can either deploy the configurations to the devices or cancel the provisioning operation.

The circuit should be added to the list in the **Circuits/VCs** tab in the **Network Topology** window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Circuit Section Reference for OTN Circuit Types

The following table lists and describes the attributes that define the OTN circuit types.

Table 6: Circuit Section Reference—OTN Circuit Types

Attribute	Description	Enabled
Circuit Properties		
Bandwidth	Bandwidth required to provision the OTN circuit. See Table 8: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits for the mapping of values in the Bandwidth, and Service Type fields.	For all OTN circuit types.
A-End Open Ended	Check this check box to create an open-ended circuit, in which the source end point is connected to an ODU subcontroller, instead of a client payload controller. **Note** Checking this checkbox will not deploy ODU subcontrollers on the Cisco NCS 4000 devices. You must configure the ODU subcontrollers on the Cisco NCS 4000 devices before adding the devices to Cisco EPN Manager. For more information about the open ended ODU UNIs and how to configure ODU subcontrollers on Cisco NCS 4000 devices, see Open Ended ODU UNI.	For ODU UNI circuit type when the Bandwidth field is set to ODU0, ODU1, ODU2, or ODU2E.

Attribute	Description	Enabled
Z-End Open Ended	Check this check box to create an open-ended circuit, in which the destination end point is connected to an ODU subcontroller, instead of a client payload controller. **Note** Checking this checkbox will not deploy ODU subcontrollers on the Cisco NCS 4000 devices. You must configure the ODU subcontrollers on the Cisco NCS 4000 devices before adding the devices to Cisco EPN Manager. For more information about the open ended ODU UNIs and how to configure ODU subcontrollers on Cisco NCS 4000 devices, see Open Ended ODU UNI.	For ODU UNI circuit type when the Bandwidth field is set to ODU0, ODU1, ODU2, or ODU2E.
Service Type	Service types supported for the selected bandwidth. See Table 8: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits for the mapping of values in the Bandwidth and Service Type fields.	For ODU UNI circuit type.
Route Properties		
Bit Rate	Total number of bits per second.	For all OTN circuit types (except ODU UNI Hairpin) when the Bandwidth field is set to ODUFLEX.
Framing Type	The elementary signal of the requested service. Values are: • CBR—Constant bit rate. • GFP-F-Fixed—Fixed and frame mapped generic framing procedure.	For all OTN circuit types (except ODU UNI Hairpin) when the Bandwidth field is set to ODUFLEX.
Record Route	Check this check box to record the circuit route.	For all OTN circuit types (except ODU UNI Hairpin).

Endpoint Section Reference for OTN Circuit Types

The following table lists and describes the attributes that define the protection type and path options for OTN circuit types.

Table 7: Endpoint Section Reference—OTN Circuit Types

Attribute	Description	Enabled
Endpoints		
Device Name	A end and Z end devices of the circuit. **Note** For ODU UNI Hairpin circuits, both A end and Z end will be the same device but with different termination points.	For all OTN circuit types.
Interface	Interface names for the A end and Z end devices.	For ODU UNI circuits.
Termination Point	Termination point for the cards.	For OPU over ODU and ODU UNI Hairpin circuits.
Protection Type	Protection type for the OTN circuit. Values are: • 1+0—Unprotected card. If a failure is detected in the working path, it results in loss of data. • 1+1—Both primary and secondary path carry traffic end to end and the receiver receives and compares both the traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path. • 1+R—When the primary path fails, the restored path is calculated and traffic is switched to the restored path. If the primary path is non-revertible, the restored path becomes the new primary path. • 1+1+R—Both primary and secondary path carry traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path. The restored path is calculated and traffic is switched to the restored path. If the primary or secondary path is non-revertible, the restored path becomes the new primary or secondary path. **Note** This protection type is not supported for Cisco NCS 4000 series devices.	For all OTN circuit types (except ODU UNI Hairpin).
Diverse From Tunnel ID	Select a tunnel to ensure that it is not used by the circuit you are provisioning. This is to ensure that if there is a failure in a tunnel, the same tunnel is not used by another circuit.	For all OTN circuit types(except ODU UNI Hairpin).
Working Path,**Protected Path**, and **Restored Path**		

The Protected Path field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+1 or 1+1+R.

The Restored Path field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+R or 1+1+R.

Provision Circuits/VCs

Bandwidth and Service Type Value Mapping for ODU UNI Circuits.

Attribute	Description	Enabled
Type	Choose the type of working path or protected path for the circuit. Values are Dynamic and Explicit.	For all OTN circuit types (except ODU UNI Hairpin).
New	Check this check box to create a new explicit working or protected path for the circuit.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit.
Select Existing EP	Choose an existing explicit working or protected path for the circuit.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit and the New check box is unchecked.
New Name	Enter a name for the explicit path that you are creating. In the table below the New Name field, click the '+' button to add a new row to the table, and then select a device and an explicit path controller as the interface for the device.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit and the New check box is checked.

Protection Profile

The Protection Profile field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+1, 1+R, or 1+1+R and a valid A end device is selected.

| Protection Profile | The profile used to manage the protection of the circuit. This protection profile must be configured on the A end node of the circuit.

Note   You can enter the protection profile that was configured on the device.

The details of the protection profile such as the protection type, SNC, hold off, wait to restore, and whether the circuit is revertive are displayed. | |

Bandwidth and Service Type Value Mapping for ODU UNI Circuits.

The following table maps the values in the Bandwidth and Service Type fields for the ODU UNI circuits

Table 8: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits

Bandwidth	Service Type
ODU0	• Ethernet OPU0 GMP
ODU1	• OTN OPU1 • Sonet OPU1 BMP • SDH OPU1 BMP
ODU1E	• Ethernet OPU1e BMP • OTN OPU1e
ODU1F	• OTN OPU1f
ODU2	• Ethernet OPU2 GFP_F • Ethernet OPU2 GFP_F_EXT • Ethernet OPU2 WIS • OTN OPU2 • Sonet OPU2 AMP • Sonet OPU2 BMP • SDH OPU2 AMP • SDH OPU2 BMP
ODU2E	• Ethernet OPU2e BMP • OTN OPU2e
ODU2F	• OTN OPU2f
ODU4	• OTN OPU4 • Ethernet OPU4 GFP_F • Ethernet OPU4 GMP
ODUFLEX	• OTN OPUFlex • Ethernet OPUFlex GFP_F

Create and Provision an ODU Circuit

To create and provision an ODU circuit:

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 18.

Step 1   From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2   Click **Device Groups**, and then select the location in which you want to create the ODU circuit.

Step 3   Close the **Device Groups** popup window.

Step 4   In the **Network Topology** window, click **Circuits/VCs**.

Step 5   Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

               You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6   From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area.

Step 7   In the **Service Type** area, choose **ODU**.

Step 8   If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9   Click **Next** to go to the **Customer Section** page.

Step 10   (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11   Enter the circuit name and its description in the **Customer Section** page.

Step 12   Click **Next** to go to the **Circuit Section** page.

Step 13   Choose one of the following protection type for the circuit:

- None—No protection type for the circuit.
- 1+1—Both primary and secondary paths carry traffic end to end and. The receiver receives the traffic from both primary and secondary paths, and compares both the traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path.

      Note   If you have selected 1+1 as the protection type, the Connection Mode is set to SNC-N, by default.

Step 14   Choose the required Reversion Time and Hold off Timer for the circuit.

      Note   These fields are available only if you have selected 1+1 as the protection type.

Step 15   Click **Next** to go to the **Endpoint Section** page.

Step 16   Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Termination Point columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.

      Note   When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.

Step 17   (Optional) Click **Calculate Path** to verify if there is a valid working path between the selected endpoints. If a valid working path exists between the selected endpoints, the path appears with a 'W' label on the topology map. If a valid working path does not exist between the selected endpoints, a Path Calculation Result section appears that displays the reason why a working path cannot be established between the selected endpoints.

Step 18   Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

               The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Provision L3VPN Services

Supported L3VPN Services

An MPLS Layer 3 VPN creates a private IP network. The customer connects to the network via customer edge (CE) routers, which act as IP peers of provider edge (PE) routers.

Virtual Routing and Forwarding (VRFs)

On the PE, Virtual Routing and Forwarding (VRF) instances act as virtual IP routers dedicated to forwarding traffic for the L3VPN service. The VRFs learn the routes to each other via the Multi-Protocol Border Gateway Protocol (MP-BGP), and then forward traffic using MPLS.

A VPN is comprised of at least one but typically several VRFs. Cisco EPN Manager uses the VPN ID to discover which VRFs together form a single VPN. If Cisco EPN Manager discovers an existing network where no VPN ID has been provisioned, it takes all VRFs with the same name and associates them into one VPN. For VPNs created using Cisco Prime Provisioning, which uses a naming convention with version number prefixes and different suffixes, Cisco EPN Manager will recognize the different VRFs as belonging to one VPN.

In general there is a regular expression which can be configured to allow for varying naming convention.

Route Targets (RTs)

The connections between VRFs are defined using Route Targets (RTs) that are imported and exported by the VRFs. Cisco EPN Manager makes it easy to set up a full mesh of connections, and automatically allocates the route target to be used. The route target consists of a prefix which is either an AS number or an IPv4 address, for example, a full mesh prefix, 100 [681682]. The prefix can be selected from the existing BGP autonomous system (AS) numbers in the network, or it can be entered manually. The second number following the prefix is allocated automatically by Cisco EPN Manager.

Alternatively or in addition to the full mesh, it is possible to manually select route targets. During VPN creation, there is an initial screen where you type in the route targets to be used within a VPN, and then for each VRF you can select which route targets you import and export. You also specify for which address family (IPv4 or IPv6) you will use the route target. This can be used for example to configure extranets, by importing route targets used in other VPNs.

Route Redistribution

The routes that are exchanged between the PE and the CE have to be redistributed into the MP-BGP routing protocol so that remote endpoints can know which prefixes can be reached at each VRF. To control route redistribution, Cisco EPN Manager allows you to define the required protocol (Static, Connected, or RIP), the protocol's metric value, and optionally the applicable route policy.

Endpoints

Cisco EPN Manager supports the creation of IP endpoints on Ethernet subinterfaces. It supports selecting untagged encapsulation, or specifying an outer and optionally an inner VLAN, with 802.1q or 802.1ad encapsulation. You can specify both IPv4 and Ipv6 addresses at an endpoint. You can also specify the BGP neighbor details to provision BGP neighbors between the CE and PE.

For information on how to provision L3VPN service using Cisco EPN Manager, see, .

L3VPN Provisioning Features and Limitations

Cisco EPN Manager supports the following L3VPN features:

- Creation of VRFs.

- Automatic allocation of VPN IDs and Route Target IDs.

- Automatic allocation of route distinguishers.

- Discovery of VPNs consisting of several VRFs, based on multiple criteria (VPN ID, common name, and Prime Provisioning naming conventions).

- You can select devices for L3VPN provisioning using the Point and Click method of provisioning.

- Definition of IP endpoints attached to a VRF. Associating Ethernet subinterfaces with VRFs.

- Provisioning of BGP neighbors between the CE and PE.

- Attaching QoS profiles to the endpoint interfaces.

- Adding new VRFs to existing VPNs.

- Modifying VPNs and associated VRFs created and deployed (or discovered and promoted) using Cisco EPN Manager.

- Overlays in the Network Topology for L3VPN services.

- Promotion of L3VPN services discovered directly from the device. This further helps in modifying and deleting discovered services.

- Using route targets with OSPF dual AS routing.

- Using integrated routing and bridging to provision L3VPN services using BDI/BVI interfaces (subinterfaces).

- Associating IP Service Level Agreements (SLAs) and CLI templates with L3VPN services.

- Route redistribution between the PE-CE link and the MP-BGP core using connected, static, RIP, or OSPF routes.

- Provisioning L3VPN services using LAG interfaces.

Cisco EPN Manager has the following L3VPN limitations:

- VRFs are supported only on Cisco ASR1000, Cisco ASR9000, Cisco ASR90X, Cisco ASR 920X, and Cisco ASR901S devices.

- You cannot provision multicast VPNs. Only unicast VPNs are supported.

- While creating the L3VPN service, you can add only up to five VRFs to the VPN. More VRFs can later be added to the VPN using the Modify VRF and Add VRF options.

- Only one VRF per device is supported. You can create multiple VRFs but on different devices either with the same VRF name or with different VRF names.

- Route policies can be selected but cannot be defined within the L3VPN service.

- Only BGP PE-CE routing protocol is supported.

- There is no support for multiple attached PEs, and so there is no Site of Origin and HSRP support.

- IP SLA operations can be associated with VRFs only during service creation and not during service modification.

- Deleting an L3VPN service deletes the IP SLA operations associated with the service from the device. And the associated operations that are deleted will not be available for future usage.

- The Integrated Routing and Bridging (IRB) is not supported for Cisco Catalyst 6500 series switches..

Prerequisites for L3VPN Provisioning

For more information about implementing L3VPNs, see Implementing MPLS Layer 3 VPNs.

Before you begin provisioning L3VPN services, ensure that the following pre-requisites are followed.

Following are the prerequisites for provisioning an L3VPN service:

- BGP must be set up on all devices. Typically all devices must communicate with each other via a pair of route reflectors.
- Pre-configuration changes required to set up BGP:

Configure the BGP router-id as shown in the example below:

```
router bgp 65300
    bgp router-id 1.1.1.1
```

Set Vpn4 and Vpn6 as the parent address family using these commands:

```
router bgp 100
address-family vpnv4 unicast
address-family vpnv6 unicast
```

- MPLS reachability must be set up between the devices. MPLS core network configuration must be set up.
- Inventory collection status for the devices on which the L3VPN services will be provisioned must be 'Completed'. To check the status of devices, go to **Inventory > Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- (Optional) Customers must be created in the system so that you can associate the L3VPN service to a customer during L3VPN service provisioning. To create and manage customers, choose **Inventory > Other > Customers**.

L3VPN Service Discovery

Cisco EPN Manager associates multiple VRFs into a single VPN using multiple criteria:

- If VRFs were configured with a VPN ID: then the VPN service is discovered using the VPN ID to identify the VRFs that belong to the same VPN. If you have VPNs that you need to discover, where differing VRF names are used within one VPN, then configuring a common VPN ID in all the VRFs enables Cisco EPN Manager to discover the VRFs as a single VPN.

  In cases where no more than one VRF is created per device, it is common practice to simply use the same VRF name everywhere across the VPN. If Cisco EPN Manager sees multiple VRFs with the same name and no VPN ID, then it considers them as a single VPN, and the VPN name will be the name of the VRFs.

- If VPNs that were originally provisioned using Prime Provisioning: Cisco EPN Manager is also aware of the Prime Provisioning VRF naming convention. The naming convention used by Prime Provisioning is in the format:

  V<number>:<VPN name><optional suffix, one of -s -h -etc>

  VRFs with the same names and numbers will belong to the same VPN. For example these are VRFs belonging to a VPN called 'ABC':

  V1:ABC, V2:ABC, V4:ABC-s, V22:ABC-h, V001:ABC, etc.

- If the VRF has no VPN ID: and has a unique name that doesn't match other names according to the Prime Provisioning convention, it will be placed into a VPN on its own. The name of the VPN will be the name of the VRF.

The Prime Provisioning naming convention feature is driven by a regular expression that is embedded in the product. If configuring a VPN is not an option for you and you have a naming convention that could be matched with a regular expression, it is possible to change it. To change the regular expression, please contact your Cisco Advanced Services representative.

Create and Provision a New L3VPN Service

The process of creating and provisioning a unicast L3VPN involves:

- (Optional) Associating a customer to the VPN.

- Defining the attributes that influence how traffic that is delivered over the L3VPN and through its endpoints will be treated.

- Specifying the endpoints and route redistribution values of the L3VPN.

- (Optional) Configuring IP Service Level Agreements (SLAs) operation to monitor end-to-end response time between devices using IPv4 or IPv6.

- (Optional) Associating user defined CLI templates with the L3VPN service.

Note: Only Unicast L3VPN services are supported in this release.

To create a new L3VPN service:

Step 1   From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2   From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

Step 3   Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar.

The Provisioning Wizard opens in a new pane to the right of the map. You can also access the L3VPN Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.

Step 4   From the **Technology** drop-down list, select **L3VPN**. A list of supported L3VPN service types is displayed.

Step 5   In the **Service Type** section, choose **Unicast** and click **Next** to enter the customer and service details. In this release, only service type Unicast L3VPN is supported.

Step 6   (Optional) Select the customer that you want to associate with the VPN. If there are no customers in the drop-down list, you can go to **Inventory > Other > Customers** to create the customer and return to this step.

Step 7   Specify the basic L3VPN parameters:

a)   Use the **Activate** check box to specify whether the service must be in active (check box enabled) or inactive (check box disabled) state. The Active state enables traffic to pass through the circuit and automatically sets the Service State for all associated IP endpoints to True. In the Inactive state, you can choose to set the service state for IP endpoints to true or false.

b)   Provide a unique name for the service and optionally enter a description

c)   In the **IP MTU** field, enter a value between 1522 (default) and 9216. The service MTU is the size in bytes of the largest IP packet that can be carried unfragmented across the L3VPN. It does not include layer 2 headers.

The configured interface MTU is the service MTU plus the size of any layer 2 headers. For Ethernet, this will add 14 bytes plus 4 bytes per VLAN header.

The value of the UNI MTU depends on the service MTU and outer and inner VLAN values:

- If both outer and inner VLANs are present, then the UNI MTU value is greater than the Service MTU + 14 + (4*2)

- If only the outer VLAN is present, then the UNI MTU value is greater than the Service MTU + 14 + (4 *1)

- If no VLANs are present, then the UNI MTU value is greater than the Service MTU + 14

d)   (Optional) To create a full mesh topology for this service, select the **Create Full Mesh** check box and enter the full mess prefix manually or select a value from the **Full Mesh Prefix** drop-down menu. The available options depend on the full mesh prefix values discovered from the selected device.

Step 8   Use the **Route Target Allocation** section to manually specify the route target address families (**IPv4, IPv6, or Both**) and their associated route target values. You can create multiple route targets for the L3VPN service. These route targets can be associated with any VRF that you attach to this L3VPN service in the following steps.

Note   The route targets associated with a VRF must also be associated with the L3VPN the VRFs belong to.

Step 9   In the **Deployment Action** drop-down menu, specify the task that must be taken up when the service creation process is completed. Your options are:

- **Preview**: allows you to review the configuration that is generated before it is deployed to the device.

- **Deploy**: allows you to deploy the configuration to the relevant devices immediately upon completion.

Step 10   Click **Next** to associate VRFs to the L3VPN service.

Step 11   Select the required VRFs from the **VRFs** drop-down menu or add a new VRF as explained below, and then click **Next**. During L3VPN service creation, you can associate up to five VRFs with the VPN. To associate more VRFs to the VPN, see Add and Copy VRFs to an L3VPN Service, on page 51. To create a new VRF:

1. Click the '+' icon to add the VRF details manually. To auto populate the VRF details, click the respective device on the map. The device details and a new name for the VRF are automatically populated on the Add VRFs page.

2. To manually specify the VRF details, select the required device from the **Device** drop-down list. You can then manually enter the VRF name and description, and check the **RD Auto** check box.

   Note   If multiple VRFs are created on the same device, you must name them differently to ensure that they are not part of the same VPN. You cannot create multiple VRFs with the same names on the same device.

Step 12   Specify the IPv4 and IPv6 route targets and route distribution details:

1. Route Targets: Select the route targets for this VRF from the **Route Target** drop-down menu. The options in this drop-down menu are available based on the route targets associated with this service in Step 7.

2. Select the direction in which the route targets must be applied. Depending on the device you select, choose **Import**, **Export**, **Both**, or **None**.

   Choose the directions depending on the type of device that is selected. For example, for Cisco IOS-XR devices, you cannot choose 'None' as the route target direction.

3. In the **Route Policy** drop-down list, specify the import export policy for the route targets.

4. In the **Route Distribution** section, specify the protocol that must be associated with the VRF, the protocol's metric value, and the relevant route policies.

   • **Protocol**- Choose the source protocol from which routes must be redistributed. Your options are Static, Connected, RIP, and OSPF.

   • **Metric**- (Optional) Enter a numeric value for the metric which is used when redistributing from one routing process to another process on the same router.

   • **Routing Process**- (applicable only to OSPF and RIP) Specify the unique numerical value that identifies the instance of the routing process on the device.

   • **Route Policy**- (Optional) Select one of the route policies present on the selected device. You cannot create route policies using Cisco EPN Manager.

   • **Route Match Type** (applicable only to OSPF)- Specify the match type that must be associated with the selected route policy. Your options are: Internal, External, External 1, External 2, NSSA External, NSSA External 1, NSSA External 2, NSSA, Level 1, Level 2, and Level Inter Area.

Step 13   Specify the IP endpoints and UNIs values manually as follows:

   • If the endpoint interface has already been configured as a UNI, uncheck the **New UNI** check box and select the required UNI from the **UNI Name** drop-down list.

   • To create a new UNI:

   1. Select the **Create New UNI** check box.

   2. In the **UNI Name** field, enter a unique name for the UNI.

   3. In the **Device** drop-down, select the device, its required interface, and provide a description for the UNI.

   4. Check the **Service Multiplexing** check box to enable more than one L3VPN or Carrier Ethernet service to be supported at the UNI.

   5. Specify the IP Maximum Transmission Unit, the speed and duplex settings for the UNI.

6. Choose the UNI QoS profiles for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. If you select a UNI QoS profile, you cannot add individual QoS policies to the service endpoint in the upcoming steps. If you want to add specific QoS policies to the endpoint, leave the UNI Ingress and Egress QoS Profile fields blank.

Note You can choose two different discovered QoS profiles for the ingress and egress directions, however, in case of user defined QoS profiles, only a single QoS profile can be chosen for both directions.

7. Select **Enable Link OAM** to enable IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch.

8. Select **Enable Link Management** to enable the customer access switch to get information about this UNI, VLAN IDs, services on the UNI, and so on.

For a detailed description of the fields and attributes in the UNI table, see New UNI Details Reference, on page 12.

Step 14 Specify the service end point to be associated with the L3VPN by providing the following details, and then click **Next**:

• **VRF Name**: Choose one of the available VRFs that can be associated with this VPN.

• **IPv4 and IPv6 address**: Enter the IP addresses and network masks of the service end point. The masks can be entered simply as an integer that represents the length of the network mast (or in CIDR format).

• **VLAN and Inner VLAN**: Enter the inner and outer VLAN identifiers using integers between 1 and 4094. Inner VLAN is the identifier for the second level of VLAN tagging.

• **QoS Policy**: (Optional) Select the QoS policy that must be applied to the service endpoint. This field is disabled if you have associated UNI Ingress/Egress QoS profiles to the service in the above step. For information on creating QoS profiles, see Configure Quality of Service (QoS).

Note You can choose two different discovered QoS policies for the ingress and egress directions, however, in case of user defined QoS policies, only a single QoS policy can be chosen for both directions.

• **Service State**: Specify whether the service state for associated IP endpoints must be set to true or false. If the L3VPN is in Activate state (specified in Step 6 above), this check box is disabled and all service state values are automatically set to True.

• **Use Integrated Routing & Bridging**: Specify whether the VRF and IP addresses must be configured under the sub-interfaces or under the BVI (virtual) interfaces.

Note This check box is enabled only when you select devices such as, Cisco ASR 90XX devices, that support integrated routing and bridging.

Step 15 (Optional) Enter the BGP neighbor details described in the table below and then click **Next**.

BGP Neighbor Parameters	Descriptions
Device	Specify the device where the VRF will be placed for the selected VPN.
VRF	Specify the VRF used to reach this neighbor.
IP address	Enter the IP address of the neighbor.

BGP Neighbor Parameters	Descriptions
Neighbor AS	Enter the autonomous system number of this neighbor, which is the unique identifier used to establish a peering session with a BGP neighbor.
Ingress RP	Enter the route policy applied to any BGP routes received from this neighbor.
Egress RP	Enter the route policy applied to any routes sent to this neighbor.
Local AS	(Optional) Enter the unique local identifier used to establish a peering session with a BGP neighbor.
AS Action	(Optional) Select one of the following action types that must be associated with the local autonomous-system (AS) number: • **Prepend**: Use this option to configure BGP such that it prepends the AS number to routes received from the neighbor. • **No Prepend**: Use this option to configure BGP such that it does not prepend the AS number to routes received from the neighbor. • **No Prepend, Replace AS**: Use Replace AS to prepend only the local AS number (as configured with the ip-address) to the AS_PATH attribute. The AS number from the local BGP routing process is not prepended. • **No Prepend, Replace AS, Dual AS**: Use the Dual AS option to configure the eBGP neighbor to establish a peering session using the AS number (from the local BGP routing process) or by using the AS number configured with the ip-address argument (local-as).

Step 16   (Optional) Select existing IP SLA parameters from the list, or specify the IP SLA operation parameters described in the table below and then click **Next**.

IP SLA Settings	IP SLA Parameters	Descriptions
Operation Settings	Name	Enter a unique name to identify the IP SLA operation for the selected L3VPN service.
	Type	Select the type of IP SLA operation that must be generated for the devices participating in this L3VPN service. Your options are: • **UDP Echo**: Configures an IP SLAs User Datagram Protocol (UDP) Echo operation to measure response times and to test end-to-end connectivity between a Cisco device and devices using IPv4 or IPv6. • **ICMP Echo**: Allows you to measure end-to-end network response time between a Cisco device and other devices (source and destination values, as described below) using IPv4 or IPv6. With an IP SLA operation of type ICPM Echo, you cannot associate the 'Connection Loss' action variable. • **ICMP Jitter**: Configures the Internet Control Message Protocol (ICMP) Jitter operation which provides the capability to generate a stream of ICMP packets between a Cisco IOS device (source) and any other IP device (destination) to gather network performance-related statistics. Statistical measurements for the IP SLAs ICMP jitter operation include latency, round-trip time, jitter (interpacket delay variance), and packet loss. • **UDP Jitter**: Configures the UDP jitter operation which analyzes round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic in IPv4 or IPv6 networks.
	Source	Specify the device which acts as the source point from which the IP SLA configuration is generated. The IP SLA responses are generated based on the connectivity between this source device and the target device. The VRF values for this operation are automatically selected based on your Source selection.
	Source Port	Enter a numeric value between 0 and 65535 to specify the source port value for which the IP SLA operation must be configured.
	Destination	Specify the device which acts as the target point from which the IP SLA configuration is generated. The IP SLA responses are generated based on the connectivity between the source device and this target device.
	Destination Port	Enter a numeric value between 0 and 65535 to specify the destination port value for which the IP SLA operation must be generated.
	VRF	The VRF details are automatically selected based on the device you specify as the IP SLA operation Source.

IP SLA Settings	IP SLA Parameters	Descriptions
Reaction Settings	Action Variable	Select the variable based on which the IP SLA reactions must be triggered. For example, when a monitored value exceeds or falls below a specified level, or when a monitored event (such as a timeout or connection loss) occurs. • **Connection Loss**: Indicates that an event must be triggered when a connection loss occurs. This value is not displayed if you select ICPM Echo as the type of operation. • **Round Trip Time**: If you choose this action variable, you need to enter the **Upper Threshold Value** and the **Lower Threshold Value** which indicates that an event must be triggered when a monitored value exceeds or falls below the upper and lower threshold values that you specify. • **Time Out**: Indicates that an event must be triggered after a given set of consecutive timeouts occur. • **Verify Error**: Indicates that an event must be triggered after an error of type 'VerifyError' occurs.
	Action Type	Select one of the following actions that must be taken based on the conditions set in the Action Variable field: • **None**: No action is taken. • **Trap and Trigger**: Triggers both an SNMP trap and starts another IP SLAs operation when the violation conditions are met, as defined in the Trap Only and Trigger Only options below. • **Trap Only**: Sends an SNMP logging trap when the specified violation type occurs for the monitored element. • **Trigger Only**: Changes the state of one or more target operation's Operational state from 'pending' to 'active' when the violation conditions are met. A target operation will continue until its life expires (as specified by the target operation's configured lifetime value). A triggered target operation must finish its life before it can be triggered again.
	Threshold Type	

IP SLA Settings	IP SLA Parameters	Descriptions
		Select the threshold type based on which the IP SLA events are generated. • **Average**: If you choose this threshold type, enter the **N Value** which specifies that an event must be triggered when the averaged total value of N probes is reached either when specified upper-threshold value is exceeded, or when it falls below the lower-threshold value. • **Consecutive**: If you choose this threshold type, enter the **Consecutive Values** as part of the reaction settings. This threshold type triggers an event only after a violation occurs a specified number of times consecutively. For example, if you enter 5 as the consecutive value, the consecutive violation type is used to configure an action to occur after a timeout occurs 5 times in a row, or when the round-trip-time exceeds the upper threshold value 5 times in a row. • **Immediate**: Triggers an event immediately when the value for a reaction type (such as response time) exceeds the upper threshold value or falls below the lower threshold value, or when a timeout, connection loss, or verify error event occurs. • **Never**: Never triggers an event. • **X out of Y occurrences**: If you choose this threshold type, enter the **X Values** and **Y Values** to specify the number of occurrences. This triggers an event after some number (x) of violations within some other number (y) of probe operations (x of y).
Simple Schedule	-	Enter the scheduling parameters for an individual IP SLAs operation by entering the following values: • **Frequency**: Enter the elapsed time within which the operation must repeat, in seconds. • **Life Time**: Enter the overall time until when the operation must be active, in seconds. A single operation repeats at the specified frequency for the lifetime of the operation. • **Age Out**: Enter the length of time to keep an operation active, in seconds. For example, an age out value of 43200 will ensure that the operation will age out after 12 hours of inactivity. • **Start Now** and **Start After**: Enable the Start Now check box to schedule the IP SLA operation to be executed immediately on Save. Or use the Start After field to specify the number of minutes after which the operation can be executed.

Step 17   (Optional) Use the Service Template page to append a template with additional CLI commands that will be configured on the devices participating in the service. See Extend a Circuit/VC Using Templates, on page 80 for more information.

Step 18   When you have provided all the required information for the service, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the L3VPN attributes. Otherwise, the configurations will be deployed to the devices immediately.

In case of a deploy failure on even a single device that is part of the service, the configuration is rolled back on all devices participating in the service. To delete the endpoints associated with the service, see, Delete an L3VPN Service Endpoint. To add more VRFs to this L3VPN service, see Add and Copy VRFs to an L3VPN Service, on page 51.

Example Configuration: Provisioning an L3VPN Service

The following are examples of the configuration deployed to a Cisco ASR 9000 device with the following parameters:

- Creation of VRF and IP addresses (both IPv4 and IPv6) under the BDI (virtual) interface.

- Redistribution of OSPF protocol to the BGP protocol.

Example: Provisioning an L3VPN service on a Cisco ASR 9000 device's BVI enabled interface (sub-interface).

```
vrf vrfrbvibdi9k
vpn id aaaaaa:21
address-family ipv4 unicast
  import route-target
    6:55
address-family ipv6 unicast
  import route-target
    6:55
  export route-target
    6:55
interface GigabitEthernet0/0/0/17
  no shutdown
  exit
interface GigabitEthernet0/0/0/17.1
  encapsulation dot1q 1198
  shutdown
interface BVI 1
  vrf   vrfrbvibdi9k
  ipv4 address 88.7.6.4 255.224.0.0
l2vpn
  bridge group BDI1
    bridge-domain 1
      routed interface BVI 1
      interface GigabitEthernet0/0/0/17.1
router bgp 140
  vrf  vrfrbvibdi9k
    rd auto
    address-family ipv6 unicast
    address-family ipv4 unicast
      exit
    exit
  exit
```

Example: Using a BVI enabled interface for provisioning an L3VPN service with OSPF route distribution (using dual AS):

```
vrf definition VRF2-2VRF-2UNI-BDI
  vpn id AAAAAA:2
  rd 532533:2
  address-family ipv4
    route-target import 6:5
    route-target export 6:5
  address-family ipv6
    route-target export 6:5
```

```
interface GigabitEthernet0/0/0
  duplex full
  service instance 2 ethernet
    encapsulation dot1q 761
    bridge-domain 14
    shutdown
  exit
interface BDI14
  vrf forwarding VRF2-2VRF-2UNI-BDI
  ip address 5.44.3.7 255.255.0.0
router bgp 120
  address-family ipv4 vrf VRF2-2VRF-2UNI-BDI
    neighbor 55.4.3.2 remote-as 71
    neighbor 55.4.3.2 activate
    redistribute rip metric 6
    neighbor 55.4.3.2 local-as 387
  address-family ipv6 vrf VRF2-2VRF-2UNI-BDI
    neighbor c5::98 remote-as 50
    neighbor c5::98 activate
    redistribute ospf 65 match external metric 2
    neighbor c5::98 local-as 324 no-prepend replace-as dual-as
    exit
  exit
```

View L3VPN Service Details

Using Cisco EPN Manager, you can view the detailed information about an L3VPN service in the following ways:

- **Using the Circuit/VC 360 View:** The Circuit/VC 360 view provides detailed information available for a specific L3VPN created using Cisco EPN Manager. See View Circuit/VC Details. The different parameters associated with the L3VPN service are displayed in three different tabs: Summary, VRFs, Site Details, and BGP Neighbors.

- **Using the Network Topology and Service Details View:** The Network Topology window presents a graphical, topological map view of devices, the links between them, and the active alarms on the devices or links. It also enables you to visualize L3VPNs within the displayed topology map.

  - To view a complete list of L3VPNs and its details, see View a Device Group's Circuits/VCs List in the Topology Window. See, Circuit/VC 360 View.

  - To view the L3VPN service details for a specific device, see View Circuits/VCs In Which a Specific Device Participates.

- **Using the Alarms Table:** The Alarms Table in Cisco EPN Manager provides several ways to see, at a glance, if there are any problems with your L3VPN services. See Check Circuits/VCs for Faults.

Following are the attributes available in different L3VPN Service Details views:

Table 9: L3VPN Service Details View- Attributes and their Descriptions.

Tab Name	Attributes	Descriptions
Summary	Discovery State	Identifies whether the service was discovered from the device fully or partially or not discovered at all. This state is not defined by the service being provisioned or discovered from the network.
	Name	Unique name that identifies the L3VPN service. For services that are discovered directly from the device, this name represents the VLAN ID (numerical value) of the service.
	Customer	Customer associated with the L3VPN.
	Description	Description of the L3VPN that will help to identify the L3VPN.
	Type	L3VPN service type that is prepopulated based on the type of service that is created.
	Operational State	The state in which the L3VPN service is functioning. The states are Defined, Deploying, Failed, Discovered, and Unknown. Note- If the service state indicates Operational, Serviceability, or Primary, it represents the state of the service endpoint and not the state of the L3VPN service itself.
	MTU	The service MTU is the size in bytes of the largest IP packet that can be carried unfragmented across the L3VPN. It does not include layer 2 headers. The configured interface MTU is the service MTU plus the size of any layer 2 headers. For Ethernet, this will add 14 bytes plus 4 bytes per VLAN header.
	Provisioning Status	The service's provisioning state represents whether there is a provisioning intent for the service and, if so, its status. The possible values are: Failed, In Progress, Planned, and Succeeded.
	Serviceability State	A combination of the service's admin and operational states. The admin state is shown because it impacts service operability. The operational state is shown to quickly identify whether a service is working or not. The values are: Admin Down, Down, Up, Auto Up, Unavailable, and Partial.
VRFs	Device Name	Name of the device on which the VRF is configured.
	VRF	Name to identify the VRF.
	Description	Description of the VRF that will be configured on the device.

Tab Name	Attributes	Descriptions
Site Details (IP Endpoints)	UNI Name	Name of the UNI associated with the L3VPN.
	Device Name	Name of the device where the UNI is located.
	Interface	Name of the interface on the device which connects to the UNI.
	IP Address/Subnet Mask	The subnet mask in CIDR notation used to identify the IP address of the endpoint.
	VRF	The VRF with which this endpoint is connected.
BGP Neighbors	Device Name	The device where the VRF is located.
	VRF	The VRF used to reach this neighbor.
	IP Address	The IP address of the neighbor.
	Neighbor AS	The autonomous system number of this neighbor.
	Ingress RP	The route policy applied to any BGP routes received from this neighbor.
	Egress RP	The route policy applied to any routes sent to this neighbor.

Modify L3VPNs and VRFs

You can modify L3VPN services that are created and deployed using Cisco EPN Manager. While the full mesh prefix, QoS profiles, and RT values associated with the service can be modified, you cannot modify parameters such as the customer details, VPN name, and service MTU values associated with the service. To modify these parameters, delete the service, and re-create it with new values. You can also modify the VRFs associated with L3VPN services.

To modify L3VPN services and VRFs:

Before you begin

To modify L3VPN services that are discovered and promoted using Cisco EPN Manager, you must ensure that that the route distinguisher for the L3VPN service is specified in the format **rd device_ip:number**. For example:

```
vrf definition vdvvgfr420
  rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...
```

If the route distinguisher is specified in any other format, you will not be able to edit the service.

Step 1 Navigate to **Maps** > **Network Topology**.

Step 2 Click the **Circuits/VCs** tab, and select the L3VPN service that you want to modify.

Step 3 Click the pencil (**Modify**) icon.

Step 4 To modify the selected L3VPN, choose **Modify VPN** and click **Next**.

The Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN.

Step 5 To modify the VRFs associated with the selected L3VPN, choose **Modify VRF** and click **Next**.

The Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN. Along with modifying existing VRF parameters, you can also associate new Route Target values to the VRF.

While modifying VRFs, you cannot modify the QoS profiles associated with the UNIs, however, you can modify the QoS policies associated with the service endpoints.

Note You cannot modify the VRF name and device associated with the selected L3VPN.

Step 6 Make the required changes and click **Submit** to preview the configuration that will be deployed to the device.

Note When you modify a VPN, you cannot change the VRFs associated with the VPN. To modify the VRFs, see Add and Copy VRFs to an L3VPN Service, on page 51.

Step 7 Review your changes and click **Deploy** to deploy your changes to the device.

In case of a deploy failure on even a single device that is part of the service, the configration is rolled back on all devices participating in the service.

Step 8 To verify that your changes were saved, view the L3VPN service details. See View L3VPN Service Details, on page 48.

Add and Copy VRFs to an L3VPN Service

Using Cisco EPN Manager you can create and associate new VRFs to existing L3VPN services. You can also copy the route target and other details from existing VRFs to create new VRFs for the L3VPN service.

To associate new VRFs with an L3VPN service:

Step 1 Navigate to **Maps** > **Network Topology**.

Step 2 Click the **Circuits/VCs** tab and select the L3VPN service to which you want to associate new VRFs.

You can also access the L3VPN Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.

Step 3 Click the pencil (**Modify**) icon.

The L3VPN Provisioning wizard is displayed.

Step 4 Select **Add VRF** and click **Next**.

Step 5 Click the + icon to add the new VRF details manually. To auto populate the VRF details, click the device on the map to select it. The device details and a new name for the VRF are automatically populated on the VRF's page.

Step 6 You can copy VRF details from an existing VRF by clicking the **Copy From** drop-down list and selecting the required VRF.

Only those VRFs that are associated with the selected L3VPN are displayed along with the VRFs route target, and route redistribution details.

Step 7 Otherwise, manually specify the details of the VRFs that you want to add to the selected VPN service. For more information about the different VRF parameters, see, Create and Provision a New L3VPN Service.

Step 8 Make any required changes such as adding endpoint and BGP neighbor details and click **Submit**.

Step 9 Preview the configuration that is to be deployed to the device, make the required changes, and click **Deploy** to deploy the changes to the device.

To verify that your changes were deployed, view the selected L3VPN service's details. See View L3VPN Service Details.

For more information on modifying and deleting L3VPN services, see Delete an L3VPN Service Endpoint and Modify L3VPNs and VRFs, on page 50.

Provision Circuit Emulation Services

Summary of Cisco EPN Manager CEM Provisioning Support

Cisco EPN Manager supports the provisioning of Circuit Emulation (CEM) services. CEM provides a bridge between the traditional TDM network and the packet switched network (PSN). It encapsulates the TDM data into packets, provides appropriate header, and send the packets through PSN to the destination node. For more information, see Supported Circuit Emulation Services.

You can also assign a MPLS TE tunnel to a CEM service to allow the CEM service to traverse through the network. Use the **Preferred Path** drop-down list in the Provisioning Wizard to assign a MPLS TE tunnel for a CEM service. For more information, see CEM Service Details References, on page 54.

Prerequisites for CEM Provisioning

The following prerequisites must be met before you can provision a CEM service:

• IP/MPLS connectivity must be enabled on the originating and terminating endpoints in a CEM service.
• CEM configurations such as loopback interface and ACR groups must be configured on the devices that will be used in the CEM service. For more information, see Configure Circuit Emulation.
• Inventory collection status for the devices on which the CEM service will be provisioned must be *Completed*. To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
• Optionally, customers can be created in the system so that you can associate a CEM service to a customer during the service creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.

Create and Provision a New CEM Service

The process of creating and provisioning a CEM service in Cisco EPN Manager involves:

• Specifying endpoints of the CEM service.
• Defining the attributes that influence how traffic that is delivered over the CEM service and through its endpoints will be treated.

Before you begin

For information about the prerequisites that must be met before you can provision a CEM service, see Prerequisites for CEM Provisioning, on page 52.

Step 1	In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.
Step 2	Click **Device Groups**, and then select the location in which you want to create the CEM service.
Step 3	Close the **Device Groups** popup window.
Step 4	In the **Network Topology** window, click **Circuits/VCs**.
Step 5	Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.
	You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.
Step 6	From the **Technology** drop-down list, choose **Circuit Emulation**.
Step 7	From the **Service Type** drop-down list, choose the required CEM service type depending on the rate at which you want the circuit to transmit the data. For a list of CEM service types that Cisco EPN Manager supports, see Supported Circuit Emulation Services.
Step 8	If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.
Step 9	Click **Next** to go to the **Customer Service Details** page.
Step 10	(Optional) Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then go to the Provisioning Wizard to start provisioning the CEM service.
Step 11	Check the **Activate** check box to activate the interface associated with the service that you are provisioning.
Step 12	Enter the service name and its description.
Step 13	In the **Deployment Action** field, specify what you want to do when the CEM service creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
Step 14	Click **Next**, and then enter the A End and Z End configurations, and the transport settings for the CEM service. See CEM Service Details References, on page 54 for descriptions of the fields and attributes.
Step 15	If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, check the **Unmanaged Device** check box and provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 80 for more information.
	Note The **Unmanaged Device** check box is available only in the Z End Configurations page.
Step 16	(Optional) If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the **Template Details** page. See Extend a Circuit/VC Using Templates, on page 80 for more information.
Step 17	When you have provided all the required information for the service, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The CEM service should be added to the list in the Circuits/VCs pane in the **Network Topology** window To check the provisioning state, click on the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

CEM Service Details References

The following table lists and describes the attributes that define the CEM service types.

Table 10: Circuit Section Reference—CEM Service Types

Attribute	Description
A End and **Z End Configurations**	
Device	Name of the source and destination devices in the CEM service.
Working Path and Protecting Path	
Note The **Working Path and Protecting Path** are not available for X.21, C37.94, and EM-Voice service types.	
Port Name or Interface Name	Name of the interface on the source and destination devices in the CEM service. You can choose either the port name or the port group.
	When you choose the port name under the **Protecting Path** area, the unidirectional path switched ring (UPSR) protection mechanism is enabled.
	When you choose the port group under the **Protecting Path** area, the Automatic Protection Switching (APS) protection mechanism is enabled. For more information about how to configure protection groups, see Configure APS and UPSR Protection Groups.
Higher Order Path	When a SONET/SDH line is channelized, it is logically divided into smaller bandwidth channels called higher order paths (HOP) and lower order paths (LOP). HOP or synchronous transport signal (STS) path is used to transport TDM data of higher bandwidth. HOPs can also contain LOPs within it.
	Select the path and path mode available for the CEM service.
Lower Order Path	LOPs or virtual tributary (VT) path is used to transport TDM data of lower bandwidth.
DS0 Time Slot	Choose one or more time slots available in the DS0 group.
	Note This field is available only if you select **DS0** in the **Service Type** field.
Clocking	
The nodes in a network may be at different clock rates. Differences in timing at nodes may cause the receiving node to either drop or reread information sent to it. Clocking is essential to synchronize all nodes to the same clock rate. For more information about clocking, see Configure Clocking for CEM.	

Attribute	Description
Clock Source	Enables to recover the clock rate from single source so that all nodes can be synchronized at the same clock rate. Values are: • Internal – Clock rate recovered from the host. • Line – Clock rate recovered from the SONET/SDH line. • Adaptive Clock Recovery – Clock rate is recovered based on the dejitter buffer fill level. Due to delay variations, the dejitter buffer fill levels keep varying continuously. The TDM service clock is recovered after filtering the variations. The accuracy of the recovered clock depends on the delay variations. • Differential Clock Recovery – Clock rate is recovered from a master clock using Sync-E. For more information about how to setup the master clock for your network, see Synchronize the Clock Using Sync-E, BITS, and PTP.
Clock Rate	Select the required clock rate in bits per second (bps). For example, if the clock rate is set to 64000, you can only send 64 kbps over the serial interface. **Note** This field is available only for X.21 service type.

QOS

The list of profiles available for selection includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to Create QoS Profiles, on page 78 for information on how to create QoS profiles.

Attribute	Description
Ingress QoS Profile	Select the ingress QoS policies that are configured on the A end and Z end devices.

Unmanaged Device Details

Note   The below fields are available only for Z End Configurations.

Attribute	Description
Unmanaged Device	Check this check box to include a device that is not managed by Cisco EPN Manager and create partial service.
New Device	Check this check box to create a new unmanaged device.
Device	Choose an unmanaged device from the drop-down list. **Note** This field is available only when the **New Device** check box is unchecked.
Device Name	Enter a unique name for the new unmanaged device that you want to create. **Note** This field is available only when the **New Device** check box is checked. If the **New Device** check box is unchecked, the name of the unmanaged device that you chose in the **Device** drop-down list is populated in this field.

Attribute	Description
Device IP	Enter the IP address of the new unmanaged device that you want to create. **Note** This field is available only when the **New Device** check box is checked. If the **New Device** check box is unchecked, the IP address of the unmanaged device that you chose in the **Device** drop-down list is populated in this field.
LDP IP	Enter a valid LDP IP for the unmanaged device.
VC ID	Enter a unique Virtual Circuit (VC) ID for the unmanaged device.
Time Slot	Enter the time slot for the service. The valid range is 112. **Note** This field is available only for C37.94 service type.
Command Type	Select the PCM encoding configuration for voice port. The values are A Law and U Law. **Note** This field is available only for EM-Voice service type.
Operation	Select the number of wires used for voice transmission at this interface. The values are: • Wire 2—The audio path is full duplex with one pair of wires. • Wire 4—The audio path is full duplex with two pairs of wires. **Note** This field is available only for EM-Voice service type.
EM Signal	Select the options of signaling type configuration. The values are: • Delay Dial—The originating end goes off-hook and waits for about 200 ms, then checks to see if the destination end is on-hook. If the destination end is on-hook, the originating end sends the dial digits. If the destination end is off-hook, the originating end waits till the destination end is on-hook, and then sends the dial digits. • Immediate Start—The originating end goes off-hook, waits for a finite period of time (for example, 200 ms), then sends the dial digits to the destination end. • Wink Start—The originating end goes off-hook, waits for a temporary off-hook pulse from the destination end (which is interpreted as an indication to proceed), then sends the dial digits. **Note** This field is available only for EM-Voice service type.
EM Type	Select the type of E&M interface to which the voice port is connecting. The values are Type 1, Type 2, Type 3, Type 5, and Type To. **Note** This field is available only for EM-Voice service type.

Attribute	Description
Impedence	Select the impedance depending on the operation selected. If you selected the Operation as Wire 2, select the impedence as 600 R, Complex1, Complex2, or Complex3. If you selected the Operation as Wire 4, select the impedence as 600 R. **Note** This field is available only for EM-Voice service type.
Transport Settings	
Frame Type	This field is display-only and is auto-populated based on the CEM service type that you chose when creating the CEM service. The values are SAToP and CEP.
Payload Size	Number of bytes put into each IP packet. The valid range is 64 – 1312. The range will vary based on the device capability, level of support and the configured dejitter buffer size value. **Note** For X.21 service type, the range will vary based on the clock rate.
Dejitter Buffer Size	Determines the ability of the emulated circuit to tolerate network jitter. The valid range is 1 - 32. The range will vary based on the device capability, level of support and the configured payload size value. **Note** For X.21 service type, the range will vary based on the clock rate.
Idle pattern	Idle pattern to transmit the data when the service goes down. The valid range is 0x00 - 0xFF.
Dummy Mode	Enables you to set a bit pattern for filling in for lost or corrupted frames. The values are last-frame and user-defined.
Dummy Pattern	The bit pattern used for filling in for lost or corrupted frames. The valid range is 0x00 - 0xFF. The default is 0xFF. **Note** This field is enabled only if you choose the Dummy Mode as user-defined.
RTP Header Enabled	Check this check box to enable the Real-Time Transport Protocol (RTP) header for the CEM service.
RTP Compression Enabled	Check this check box to compress the IP header in a packet before the packet is transmitted. It reduces network overhead and speeds up the transmission of RTP.
Pseudowire Settings	
Preferred Path Type	Choose the Preferred Path Type as Bidirectional or Unidirectional.
Preferred Path	Select the MPLS bidirectional TE tunnel through which you want the CEM service to pass through. **Note** This field is available only if you selected **Bidirectional** as the Preferred Path Type.

Attribute	Description
Preferred Path (A-Z)	Select the required unidirectional tunnel through which you want the CEM service to travel from the A endpoint to the Z endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Preferred Path (Z-A)	Select the required unidirectional tunnel through which you want the CEM service to travel from the Z endpoint to the A endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Allow Fallback to LDP	Check this check box to ensure that the CEM service falls back to the default MPLS Label Distribution Protocol (LDP) when the selected preferred path goes down. **Note** This check box is available only when you select a valid MPLS TE tunnel in the **Preferred Path** field.
Send Control Word	Check this check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.

Provision MPLS Traffic Engineering Services

Summary of Cisco EPN Manager MPLS TE Provisioning Support

Cisco EPN Manager supports the provisioning of MPLS Traffic Engineering services. MPLS TE enables an MPLS backbone to replicate and expand the TE capabilities of Layer 2 over Layer 3. MPLS TE uses Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP) across the backbone. For more information, see Supported MPLS Traffic Engineering Services.

MPLS TE Service Provisioning Features

Cisco EPN Manager supports the following MPLS TE features:

- Support for constraint-based routing, and trunk admission control.

- Provision for path protection mechanism against link and node failures.

- Usage of Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP).

- Ability to advertise TE links using OSPF and ISIS.

Note For the list of devices that support the provisioning of MPLS TE tunnel, see Cisco Evolved Programmable Network Manager Supported Devices

Prerequisites for Provisioning an MPLS TE Service

The following prerequisites must be met before you can provision an MPLS TE service:

- OSPF or IS-IS must be configured on the devices that participate on the MPLS TE service.

- All links that will be used for MPLS TE service provisioning must be TE enabled.

- The TE enabled links must be operationally up.

- The tunnel's source and destination nodes must be reachable.

- MPLS reachability must be set up between the devices. MPLS core network configuration must be set up.

- Inventory collection status for the devices on which the MPLS TE service will be provisioned must be Completed. To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the **Last Inventory Collection Status** column.

- Optionally, customers can be created in the system so that you can associate an MPLS TE service to a customer during the service creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.

Create and Provision an MPLS TE Tunnel

To provision an MPLS TE tunnel:

Before you begin

For information about the prerequisites that must be met before you can provision an MPLS TE tunnel, see Prerequisites for Provisioning an MPLS TE Service, on page 59

Step 1   From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topolgy**.

Step 2   Click **Device Groups**, and then select the location in which you want to create the MPLS TE tunnel.

Step 3   Close the **Device Groups** popup window.

Step 4   In the **Network Topology** window, click **Circuits/VCs**.

Step 5   Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 6   From the **Technology** drop-down list, choose **MPLS TE**. Cisco EPN Manager displays a list of relevant service types in a **Service Type** area.

Step 7   In the **Service Type** area, choose **Unidirectional TE Tunnel** or **Bidirectional TE Tunnel**.

Step 8   If you have defined profiles to set the attributes of the different services, choose the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9   Click **Next** to go to the **Customer Service Details** page.

Step 10 (Optional) Select the customer for whom the service is being provisioned. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning wizard.

Step 11 Enter the service name and its description, and then enter the service details. See Field References for Service Details—MPLS TE Tunnel, on page 60.

> **Note** If you do not provide a service name, Cisco EPN Manager assigns a service name in the following format:
>
> • If the source and destination devices have a common tunnel ID, the service name is assigned in the <SourceDeviceName>_<TunnelId>_<DestinationDeviceName> format.
>
> • If the source and destination devices have unique tunnel IDs, the service name is assigned in the <SourceDeviceName>_<ATunnelId>_<ZTunnelId>_<DestinationDeviceName> format.

Step 12 Click **Next**, and then enter the tunnel creation parameters. See Field References for Tunnel Creation—MPLS TE Tunnel, on page 61 for descriptions of the fields and attributes.

Step 13 Click **Next**, and then enter the path constraint details. See Field References for Path Constraint Details—MPLS TE Tunnel, on page 64 for descriptions of the fields and attributes.

Step 14 Click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The service should be added to the list in the Circuits/VCs pane in the **Network Topology** window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Field References for Service Details—MPLS TE Tunnel

The following table lists and describes the attributes that define the service details for creating a MPLS TE tunnel.

Table 11: Service Details Section Reference—MPLS TE Tunnel

Attribute	Description
Enable FRR	Check this check box to enable the fast reroute feature that provides link and node protection for your MPLS TE tunnel. **Note** This check box is available only when you create a unidirectional TE tunnel.
Enable Auto Bandwidth	Check this check box to automatically assign maximum and minimum bandwidth to the TE tunnel based on the traffic. **Note** This check box is available only when you create a unidirectional TE tunnel.
Wrap Protection	Check this check box to detect mid-link failure scenarios. **Note** This check box is available only when you create a bidirectional TE tunnel.

Attribute	Description
Enable Fault OAM	Check this check box to enable the fault OAM protocols and messages that support the provisioning and maintenance of MPLS TE tunnels. **Note** This check box is available only when you create a bidirectional TE tunnel.
Enable Autoroute	Check this check box to enable autoroute for the tunnel.
Enable LockDown	Check this check box if you do not want to reoptimize the working LSP.
Enable BFD Settings	Check this check box to enable the Bidirectional Forwarding Detection (BFD) protocol. BFD provides fast forwarding path failure detection time and a consistent failure detection method.
Protection Type	Choose one of the following protection mechanism for the TE tunnel: • Working—The tunnel has only a working path. • Working+Protected—The tunnel has a working and a protected path, wherein if the working path fails, the traffic flow is automatically routed to the protected path without the links going down. • Working+Restore—The tunnel has a working and a restore path, wherein if the working path fails, the link goes down and then the traffic flow is routed to the restore path. • Working+Protected+Restore—The tunnel has a working, protected, and restore path, wherein, if the working path fails, the traffic flow is routed to the protected path. If the protected path also fails, the link goes down and then the traffic flow is routed to the restore path.
Deployment Action	Choose one of the following options to specify what you want to do when the MPLS TE tunnel creation process is completed: • Preview—Previews the configurations that will be deployed to the relevant devices before the actual deployment. • Deploy—Deploys the configurations immediately upon completion.

Field References for Tunnel Creation—MPLS TE Tunnel

The following table lists and describes the attributes that define the MPLS TE tunnel creation.

Table 12: Tunnel Creation Section Reference—MPLS TE Tunnel

Attribute	Description
Create Tunnel	
Source	Source or A endpoint of the tunnel.
Source routing Process	OSPF or ISIS routing process that is TE enabled and configured on the source endpoint selected. You can determine the router ID and loopback address configured on the source endpoint based on the OSPF or ISIS routing process.
Destination	Destination or Z endpoint of the tunnel.

Attribute	Description
Destination Routing Process	OSPF or ISIS routing process that is TE enabled and configured on the destination endpoint selected. You can determine the router ID and loopback address configured on the destination endpoint based on the OSPF or ISIS routing process.
Tunnel Setting	
Global ID	The global ID assigned to both, source and destination endpoints. This ID must be the same to bind two unidirectional tunnels into a bidirectional TE tunnel. The default value is 0. **Note** This attribute is available only when you create a bidirectional TE tunnel.
Affinity Bits	The affinity bit determines the link attribute that the bidirectional TE tunnel will use when configuring the dynamic backup paths.
Affinity Mask	The affinity mask determines which link attribute the router must check. You can use affinity bits and affinity mask to include or exclude link attributes when configuring the dynamic backup paths. If a bit in the mask is 0, the value of the associated link attribute for that bit is irrelevant. In this case, the link attribute is excluded when configuring the dynamic backup paths. If a bit in the mask is 1, the value of the associated link attribute must match the affinity of the tunnel for that bit. In this case, the link attribute is included when configuring the dynamic backup paths.
Setup Priority	Setup priority assigned to an LSP for the bidirectional TE tunnel. Based on this priority, the LSP can determine which existing tunnels or LSPs with low priority can be blocked. Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a setup priority of 0 can block any LSP with a setup priority between 1 and 7. **Note** Setup priority cannot be higher than the hold priority.
Hold Priority	Hold priority assigned to an LSP for the bidirectional TE tunnel. Based on this priority, the LSP can determine whether it must be blocked by another signaling LSP with a high setup priority. Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a hold priority of 0 cannot be blocked by another LSP.
Bandwidth Pool Type	Bandwidth pool used to manage the reservable bandwidth on each link for constraint-based routing (CBR) in MPLS TE. Values are: • Global – Regular TE tunnel bandwidth. • Subpool – A portion of the global pool. The subpool bandwidth is not reserved from the global pool if it is not in use. Subpool tunnels require a higher priority than global pool tunnels. **Note** This field is available only when you create a bidirectional TE tunnel.

Attribute	Description
Bandwidth	Bandwidth for the bidirectional TE tunnel. The value must be specified in the units of Kbps. For example, if you want to assign a bandwidth of 1000000 Kbps for the tunnel, enter the value as 1000000 Gbps. **Note** This field is available only when you create a bidirectional TE tunnel.
Auto Bandwidth Max	Cisco EPN Manager automatically assigns the maximum bandwidth for the unidirectional TE tunnel based on the traffic. However, you can change the bandwidth, if required. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** screen.
Auto Bandwidth Min	Cisco EPN Manager automatically assigns the minimum bandwidth for the unidirectional TE tunnel based on the traffic. However, you can change the bandwidth, if required. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** screen.
Bandwidth Change Frequency (Sec)	Enter the bandwidth change frequency in seconds. The valid range is between 3600 to 604800. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create unidirectional tunnels.
Adjustment Threshold	Enter the bandwidth adjustment threshold in percentage to trigger an adjustment if the largest sample percentage is higher or lower than the current tunnel bandwidth. . Adjustment threshold is the percentage of the current tunnel bandwidth and an absolute (minimum) bandwidth. Both the thresholds must be fulfilled for the automatic bandwidth to resignal the tunnel. The tunnel bandwidth is adjusted only if the difference between the largest sample output rate and the current tunnel bandwidth is larger than the adjustment thresholds. The valid range for the unidirectional tunnels that connect the Cisco IOS-XR devices is 1 to 100 and the range for the unidirectional tunnels that connect the Cisco IOS-XE devices is 1 to 99. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create unidirectional tunnels.

Attribute	Description
Overflow Threshold	Enter the overflow threshold in percentage to trigger the overflow detection. It is the percentage of the actual signalled tunnel bandwidth. When the difference between the measured bandwidth and the actual bandwidth is larger than the overflow threshold percentage for the N consecutive times (defined as the overflow limit), an overflow detection is triggered. The valid range for the unidirectional tunnels that connect the Cisco IOS-XR devices is 1 to 100 and the range for the unidirectional tunnels that connect the Cisco IOS-XE devices is 1 to 99. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create unidirectional tunnels.
Overflow Limit	Enter the number of consecutive collection periods during which the difference between the measured bandwidth and the actual bandwidth of a tunnel can exceed the overflow threshold defined for the tunnel. The valid range is 1 to 10. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create unidirectional tunnels.
Collect Bandwidth	Check this check box to collect the bandwidth information for the unidirectional tunnel. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create unidirectional tunnels.
BFD Settings	
Min Interval Multiplier	BFD uses intervals and multipliers to specify the periods at which control and echo packets are sent in asynchronous mode and their corresponding failure detection. A failure detection timer is started based on *(I x M)*, where *I* is the minimum interval, and *M* is the multiplier. **Note** These fields are available only when you check the **Enable BFD Settings** check box.

Field References for Path Constraint Details—MPLS TE Tunnel

The following table lists and describes the attributes that define the path constraint details for creating a MPLS TE tunnel.

Table 13: Path Constraint Details Section Reference—MPLS TE Tunnel

Attribute	Description
Path Type	Choose the required path for the TE tunnel. The values are **Working**, **Protected**, and **Restore**.
Working Path, **Protection Path**, and **Restore Path** Based on the value you choose in the **Path Type** field, the respective field group is available.	
Type	Choose the type of working path or protected path for the tunnel. Values are **Dynamic** and **Explicit**.
New	Check this check box to create a new explicit working, protected, or restore path for the tunnel. **Note** All the below fields are available only when you select **Explicit** in the **Type** field.
Select Existing Path	Choose an existing explicit working, protected, or restore path for the tunnel. **Note** This field is available only when you uncheck the **New** check box.
Path Name	Enter a name for the explicit path that you are creating. In the **Working Path**, **Protection Path**, or **Restore Path** table, click the '+' button to add a new row to the table, and then select a MPLS-enabled device, an explicit path controller as the interface for the device, and a path constraint type. In the path table, you can select any MPLS-enabled device except the source and destinations devices. Cisco EPN Manager supports only strict path constraint type. **Note** This field is available only when you check the **New** check box.
Working Path LSP Attribute List, **Protection Path LSP Attribute List**, and **Restore Path LSP Attribute List** Based on the value you choose in the **Path Type** field, the respective field group is available. The LSP attributes that you define here are associated with the path option you selected in the **Path Type** field and these attributes are applicable for source and destination devices. **Note** The values that are defined for a specific path option will override the values specified at the interface tunnel level. For example, if you have defined the LSP attributes for the working path, these values will override the values that you defined in the **Tunnel Settings** section at the interface tunnel level, which is common for all the path options.	
New LSP Attribute List	Check this check box to create a new LSP attribute list for the selected path type.
Existing LSP Attribute List	Choose an existing LSP attribute list for the selected path type. **Note** This field is available only when you uncheck the **New LSP Attribute List** check box.

Attribute	Description
LSP Attribute List Name	Enter a name for the LSP attribute list that you are creating. **Note** All the below fields including this field are available only when you check the **New LSP Attribute List** check box.
LSP Affinity Bits	Enter the LSP affinity bit that determines the link attribute that the bidirectional TE tunnel will use when configuring the backup paths (working, protected, or restore).
LSP Affinity Mask	Enter the LSP affinity mask that determines which link attribute the router must check when configuring the backup paths.
LSP Setup Priority	Enter the setup priority assigned to an LSP for the chosen path type. Based on this priority, the LSP can determine which existing tunnels or LSPs with low priority can be blocked. Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a setup priority of 0 can block any LSP with a setup priority between 1 and 7. **Note** LSP setup priority cannot be higher than the LSP hold priority. **Note** For Cisco IOS-XR devices, the **LSP Setup Priority** and **LSP Hold Priority** fields are not applicable.
LSP Hold Priority	Enter the hold priority assigned to an LSP for the chosen path type. Based on this priority, the LSP can determine whether it must be blocked by another signaling LSP with a high setup priority. Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a hold priority of 0 cannot be blocked by another LSP. **Note** For Cisco IOS devices, if you do not specify an LSP hold priority, Cisco EPN Manager takes the value specified in the **LSP Setup Priority** field. **Note** For Cisco IOS-XR devices, the **LSP Setup Priority** and **LSP Hold Priority** fields are not applicable.
LSP Record Route	Check the check box to record the route used by the LSP.

Create and Provision an MPLS Layer 3 Link

To provision an MPLS Layer 3 Link:

Before you begin

For information about the prerequisites that must be met before you can provision an MPLS Layer 3 Link, see .

Step 1   From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**

Step 2   Click **Device Groups**, and then select the location in which you want to create the MPLS Layer 3 Link.

Step 3   Close the **Device Groups** popup window.

Step 4   In the **Network Topology** window, click **Circuits/VCs**.

Step 5   Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 6   From the **Technology** drop-down list, choose **MPLS TE**. Cisco EPN Manager displays a list of relevant service types in the **Service Type** area.

Step 7   In the **Service Type** area, choose **Layer 3 Link**.

Step 8   If you have defined profiles to set the attributes of the different services, choose the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 77.

Step 9   Click **Next** to go to the **Link Settings** page.

Step 10   Enter a name and description for the layer 3 link.

Step 11   Choose the **A End Device**, **A End Interface**, **Z End Device**, and **Z End Interface** fields using one of the following ways:

- Click a link on the map to automatically populate the **A End Device**, **A End Interface**, **Z End Device**, and **Z End Interface** fields.
- Click a device node on the map to automatically populate the **A End Device** field. If the A End Device is connected to only one device, the **Z End Device** field is populated automatically. If the **A End Device** is connected to more than one device, you must choose the **Z End Device** manually.

Step 12   Enter the IP address and mask for the A End and Z End devices.

Step 13   Choose an L2 Discovery Protocol from the following options:

- NONE—No L2 discovery protocol to be enabled for the layer 3 link.
- CDP—Cisco Discovery Protocol to be enabled for the layer 3 link to facilitate communication between Cisco devices connected to the network.
- LLDP—Link Layer Discovery Protocol to be enabled for the layer 3 link to support non-Cisco devices and to allow for interoperability between other devices that supports the IEEE 802.1AB LLDP.
- ALL—Both, CDP and LLDP to be enabled for the layer 3 link.

Step 14   Choose the required routing protocol for the layer 3 link. The values are BGP, ISIS, and OSPF. For information about how to configure the routing protocols, see Configure Routing Protocols and Security

Step 15   (Optional) Enter a Link VLAN ID for the layer 3 link.

Step 16   (Optional) Check the **Enable MPLS TE** check box to support MPLS TE on the layer 3 link that you are provisioning.

        Note   This check box is available only when you choose OSPF or ISIS as your routing protocol.

Step 17   Click **Next**, and then enter the A End and Z End details. See Field References for A End Details and Z End Details in MPLS Layer 3 Link, on page 68 for descriptions of the fields and attributes.

Step 18   In the **Deployment Action** field, specify what you want to do when the MPLS layer 3 link creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 19   Click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The service should be added to the list in the **Circuits/VCs** tab in the Network **Topology** window. To check the provisioning state, click the i icon next to the circuit/VC name to see the Circuit/VC 360 view.

Field References for A End Details and Z End Details in MPLS Layer 3 Link

The following table lists and describes the attributes that define the MPLS Layer 3 Link.

Table 14: Field References for A End and Z End Details—MPLS Layer 3 Link

Attribute	Description	Available when the routing protocol is:
Same as A End	Check this check box if you want to have the same OSPF and MPLS-TE configurations for both A end and Z end devices. **Note** This check box is available only in the Z End Details page of the Provisioning Wizard.	BGP, ISIS, and OSPF
BGP AS Number	Choose the unique BGP autonomous system number assigned for your network.	BGP
Route Policy	Choose the routing policy to control which routes the BGP stores in and retrieves from the routing table.	BGP
Route Reflector Client	Check this check box to configure the BGP neighbor as the route reflector client for the local route reflector to advertise the available routes.	BGP
Use AIGP	Check this check box to use the Accumulated Interior Gateway Protocol (AIGP) metric attribute for the layer 3 link. The AIGP is the BGP attribute that carries the accumulated end-to-end metrics for the paths in the network.	BGP
Update Source	Choose the required source interface. **Note** This field is available only when the **Use AIGP** check box is unchecked.	BGP
ISIS Process ID	Choose an ISIS routing process ID that is available to both A end and Z end devices. For information about how to configure an ISIS process, see Configure an IS-IS Routing Protocol.	ISIS
Network	The network ID is automatically populated based on the ISIS process ID selected.	ISIS

Attribute	Description	Available when the routing protocol is:
Circuit Type	Choose the type of adjacency required for the layer 3 link from the following options: • NONE—No adjacency is established. • Level-1—Establishes a level 1 adjacency if there is at least one area address in common between the selected device and its neighbors. • Level-2-only—Establishes a level 2 adjacency on the circuit. If the neighboring device is a level 1 only device, no adjacency will be established. • Level-1-2—Establishes a level 1 and 2 adjacency if the neighbor is also configured as a level 1-2 device and there is at least one area in common. If there is no area in common, a level 2 adjacency is established.	ISIS
Level 1 Metric	Enter the metric that must be used in the SPF calculation for Level 1 (intra-area) routing. **Note** This field is available only when you choose the **Circuit Type** as **Level-1** or **Level-1-2**.	ISIS
Level 2 Metric	Enter the metric that must be used in the SPF calculation for Level 2 (inter-area) routing. **Note** This field is available only when you choose the **Circuit Type** as **Level-2** or **Level-1-2**.	ISIS
OSPF Process ID	Choose an OSPF routing process ID. For information about how to configure an OSPF process, see Configure OSPF Routing Processes. **Note** You cannot modify the OSPF routing process for the Z end device.	OSPF
OSPF Area	Enter the area in which you want to deploy the OSPF routing process.	OSPF
Metric	Enter the routing metric used by the OSPF routing process.	OSPF

Attribute	Description	Available when the routing protocol is:
BFD Template	Choose a BFD template for the layer 3 link. A BFD template defines the set of configurable parameters used by a BFD session. These include the transmit and receive timers used for BFD control and echo packets, the transmit timer interval used when the session is providing a CV function, the multiplier value, and the echo-receive interval.	BGP, ISIS, and OSPF
BFD Min Interval	Enter the minimum control packet interval for BFD sessions for the corresponding BFD configuration scope. **Note** This field is available only if you have not chosen the **BFD Template**.	BGP, ISIS, and OSPF
BFD Multiplier	Enter the BFD multiplier. This value along with the BFD minimum interval is used to determine the intervals and failure detection times for both control and echo packets in asynchronous mode on bundle member links. **Note** This field is available only if you have not chosen the **BFD Template**.	BGP, ISIS, and OSPF
BFD Fast Detect	Check this check box to quickly detect failures in the path between adjacent forwarding engines. ISIS and OSPF	
Authentication Mode	Choose the required authentication mode used to send and receive ISIS packets. **Note** The authentication fields are available only when you select Cisco IOS and Cisco IOS XE devices.	ISIS
Authentication Key Chain	Choose the authentication key chain. This enables authentication for routing protocols and identifies a group of authentication keys.	ISIS
Authentication for Send Only	Check this check box to perform authentication only for ISIS packets that are being sent.	ISIS
Password Type	Choose the password type as **Encrypted** or **Plain Text**.	BGP
Password	Type the desired password. Password is required to establish connection between two peers.	BGP
MPLS-TE		

Attribute	Description	Available when the routing protocol is:
Loopback Interface	Choose a loopback interface address for the layer 3 link. For information about how to configure a loopback interface, see Configure Loopback Interfaces.	ISIS and OSPF
TE Metric	Enter the MPLS TE tunnel metric with mode absolute.	ISIS and OSPF
TE Attributes	Enter the MPLS TE Link attribute to be compared with a tunnel's affinity bits during path selection.	ISIS and OSPF
Is Percentage	Check this check box to assign the bandwidth in percentage for the layer 3 link.	ISIS and OSPF
Global Bandwidth	Enter the regular TE tunnel bandwidth that will be reserved for the layer 3 link for CBR. For example, if you want to assign 10% as the global bandwidth for the layer 3 link, select the **Is Percentage** check box and enter the value 10 in the **Global Bandwidth** field. Whereas, if you want to assign 50 Kbps as the global bandwidth, uncheck the **Is Percentage** check box, choose Kbps from the **Bandwidth Unit** drop-down list, and then enter the value 50 in the **Global Bandwidth** field.	ISIS and OSPF
Subpool Bandwidth	Enter the subpool bandwidth that is reserved from the global pool bandwidth. For example, if you want to assign 10% as the subpool bandwidth for the layer 3 link, select the **Is Percentage** check box and enter the value 10 in the **Subpool Bandwidth** field. Whereas, if you want to assign 50 Kbps as the subpool bandwidth, uncheck the **Is Percentage** check box, choose Kbps from the **Bandwidth Unit** drop-down list, and then enter the value 50 in the **Subpool Bandwidth** field.	ISIS and OSPF
QoS		
Ingress Policy	Select the ingress QoS policies that are configured on the A end and Z end devices.	BGP, ISIS, and OSPF
Egress Policy	Select the egress QoS policies that are configured on the A end and Z end devices.	BGP, ISIS, and OSPF
Additional Settings		
Enable MPLS	Check this check box to support MPLS on the layer 3 link that you are provisioning.	BGP

Attribute	Description	Available when the routing protocol is:
Enable SyncE	Check this check box to enable Synchronous Ethernet at the interface level for the layer 3 link.	BGP, ISIS, and OSPF

Provision Serial Services

Prerequisites for Serial Circuits/VCs Provisioning

Following are the prerequisites to provision a serial circuit/VC:

- Communication between devices must be set up before you can provision a serial circuit/VC.

- Inventory collection status for the devices on which the Serial circuits/VCs will be provisioned must be "Completed". To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the Last Inventory Collection Status column.

- Optionally, customers must be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.

Create and Provision a New Serial Circuit/VC

To create a new serial circuit/VC:

Before you begin

For information about the prerequisites that must be met before you can provision a serial circuit/VC, see Prerequisites for Serial Circuits/VCs Provisioning, on page 72.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

Step 3 Click the **Circuits/VCs** tab.

Step 4 From the **Circuits/VCs** pane toolbar, click the + (**Create**) icon.

The Provisioning Wizard opens in a new pane to the right of the map.

Step 5 Select **Serial** in the Technology drop-down list.

Step 6 In the Service Type list, select the type of serial service you want to create. For information about the serial service types that Cisco EPN Manager supports, see Supported Serial Services.

Step 7	If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 77.
Step 8	Click **Next** to go to the Service Details page.
Step 9	Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
Step 10	Enter the service name and description.
Step 11	In the Deployment Action field, specify what you want to do when the circuit/VC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
Step 12	Click Next to go to the page in which you configure the endpoints. See Serial Service Details Reference, on page 73 .
Step 13	If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 80 .
Step 14	Click Next to go to the Line Settings and Pseudowire Settings page. See Serial Service Details Reference, on page 73 .
Step 15	Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the circuit/VC, do so in the Template Details page. See Extend a Circuit/VC Using Templates, on page 80 for more information.
Step 16	When you have provided all the required information for the circuit/VC, click Submit. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window.

Serial Service Details Reference

The following table lists and describes the attributes that define the serial service type.

Table 15: Circuit Section Reference—Serial Service Type

Attribute	Description
A Endpoint and **Z Endpoint Configurations**	
Device Name	Name of the source and destination devices in the serial service.
Port Name and Description	Name and description of the interface on the source and destination devices in the serial service.
QOS The list of profiles available for selection includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to Create QoS Profiles, on page 78 for information on how to create QoS profiles.	
Ingress QoS Profile	Select the ingress QoS policies that are configured on the A end and Z end devices.
Egress QoS Profile	Select the egress QoS policies that are configured on the A end and Z end devices.

Attribute	Description
Unmanaged Device Details **Note** The below fields are available only for Z Endpoint Configurations.	
Unmanaged Device	Check this check box to include a device that is not managed by Cisco EPN Manager and create partial service.
New Device	Check this check box to create a new unmanaged device.
Device Name	Enter a unique name for the new unmanaged device that you want to create. **Note** This field is available as a drop-down list if you have unchecked the **New Device** check box. You can choose an unmanaged device as your Z endpoint.
Device IP	Enter the IP address of the new unmanaged device that you want to create. **Note** This field is available only when the **New Device** check box is checked. If the **New Device** check box is unchecked, the IP address of the unmanaged device that you chose in the **Device** drop-down list is populated in this field.
LDP IP	Enter a valid LDP IP for the unmanaged device.
VC ID	Enter a unique Virtual Circuit (VC) ID for the unmanaged device.
Line Settings	
Speed	The speed of the serial link in kilo bits per second.
Data Bits	The measurement of actual data per packet that is transmitted through the serial circuit/VC. The values are 5, 6, 7, and 8.
Stop Bits	Indicates the end of communication for a single packet. The values are 1, 1.5, and 2 bits. Since the data is clocked across the lines and each device has its own clock, it is possible for the two devices to become slightly out of sync. Therefore, the stop bits not only indicate the end of transmission but also provides the network with some lenience to synchronize the different clocks. The more bits that are used for stop bits, the greater the lenience in synchronizing the different clocks, but slower the data transmission rate.
Flow Control In and Flow Control Out	Manages the rate of data transmitted between two devices when the source device transmits data at a faster rate than the destination device can receive it. It provides a mechanism for the source device to control the transmission speed, so that the destination device is not overwhelmed with data that is transmitted. The values are None, Hardware, and Software.
Flow Control Lock	Enables or disables the flow control mechanism for the serial circuit/VC. The values are True and False.

Attribute	Description
Parity	Used to check errors in serial communication. The values are: • None—No parity defined for the circuit/VC. • Even— The serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an even number of logic high bits. For example, if the data was 011, then for even parity, the parity bit would be 0 to keep the number of logic high bits even. • Odd— The serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an odd number of logic high bits. For example, if the data was 011, then for odd parity, the parity bit would be 1, resulting in 3 logic high bits. • Mark— Sets the parity bit high. This allows the receiving device to know the state of a bit which enables the device to determine if noise is corrupting the data or if the transmitting and receiving devices' clocks are out of sync. • Space—Sets the parity bit low. This allows the receiving device to know the state of a bit which enables the device to determine if noise is corrupting the data or if the transmitting and receiving devices' clocks are out of sync.
Pseudowire Settings	
Preferred Path Type	Choose the Preferred Path Type as Bidirectional or Unidirectional.
Preferred Path	Select the MPLS bidirectional TE tunnel through which you want the serial service to pass through. **Note** This field is available only if you selected **Bidirectional** as the Preferred Path Type.
Preferred Path (A-Z)	Select the required unidirectional tunnel through which you want the serial service to travel from the A endpoint to the Z endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Preferred Path (Z-A)	Select the required unidirectional tunnel through which you want the serial service to travel from the Z endpoint to the A endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Send Control Word	Check this check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.

Create and Provision a New Raw Socket Circuit/VC

To create a new Raw Socket circuit/VC:

Before you begin

For information about the prerequisites that must be met before you can provision a Raw Socket circuit/VC, see Prerequisites for Serial Circuits/VCs Provisioning, on page 72.

Step 1	From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.
	The network topology window opens.
Step 2	From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.
Step 3	Click the **Circuits/VCs** tab.
Step 4	From the **Circuits/VCs** pane toolbar, click the **+** (**Create**) icon.
	The Provisioning Wizard opens in a new pane to the right of the map.
Step 5	Select **Serial** in the Technology drop-down list.
Step 6	In the Service Type list, select **Raw Socket**. For information about the Raw Socket circuits/VCs, see Supported Serial Services.
Step 7	If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 77.
Step 8	Click **Next** to go to the Customer Service Details page.
Step 9	Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customer** to create the customer in the system, and then restart the Provisioning Wizard.
Step 10	Enter the service name and description.
Step 11	In the Deployment Action field, specify what you want to do when the circuit/VC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
Step 12	Click **Next** to go to the Server Side Configuration page. See Raw Socket Service Details Reference, on page 76 for descriptions of the fields and attributes.
Step 13	Click **Next** to go to the Client Side Configuration page. Click the '+' icon in the Raw Socket Client table to add a new row for client side configuration. See Raw Socket Service Details Reference, on page 76 for descriptions of the fields and attributes.
Step 14	Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the circuit/VC, do so in the Template Details page. See Extend a Circuit/VC Using Templates, on page 80 for more information.
Step 15	When you have provided all the required information for the circuit/VC, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window.

Raw Socket Service Details Reference

The following table lists and describes the attributes that define the Raw Socket service type.

Table 16: Raw Socket Service Type—Server Side and Client Side Configurations

Attribute	Description
Server Settings and **Client Settings**	
Device Name	Name of the devices that act as a server and client in the Raw Socket service.
Port Name	Name of the interface on the server and client devices in the Raw Socket service.
Server Address and Server Port	The IP address and the port number of the server.
Client Address and Client Port	The IP address and the port number of the client.
Connection Idle Timeout	TCP session timeout setting for the Raw Socket service. If no data is transferred between the client and server over this interval, then the TCP session closes. The client then automatically attempts to reestablish the TCP session with the server.
VRF	Virtual Routing and Forwarding (VRF) interface through which the server and client are connected to transport the data. **Note** Ensure that the VRF definition is common for both server and client.
Packetization Settings	
Packet Length	The packet length that triggers the routing device (either a server or a client) to transmit the serial data to the peer. When the device collects the specified bytes of data in its buffer, it packetizes the accumulated data and forwards it to the Raw Socket peer.
Packet Timer	Specifies the amount of time in milliseconds, the device (either server or client) waits to receive the next character in a stream. If a character is not received by the time the packet timer expires, the data the device has accumulated in its buffer is packetized and forwarded to the Raw Socket peer.
Special Char	A character that triggers the device (either server or client) to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the specified special character is received, the device packetizes the accumulated data and sends it to the Raw Socket peer.

Create Circuit/VC Profiles

Profiles contain sets of attributes specific to the different types of circuits/VCs. Once a profile is created, it will be available to all users for selection during circuit/VC creation. When a profile is selected, the Provisioning Wizard is populated with the profile attributes. Users only have to define the endpoints of the service and, if necessary, make small changes before provisioning the circuit/VC.

The types of profiles you can create mirror the types of circuits/VCs that can be provisioned.

Each profile is given a unique name, so you can create multiple profiles per circuit/VC type, depending on your needs.

To create a profile:

Step 1   Choose **Inventory > Other > Profiles** in the left navigation pane. The **Profiles** window opens, showing a table of existing profiles (if any). You can select a profile in the table to edit or delete it.

Step 2   Click **Create Profile**.

Step 3   In the Create Profile wizard, provide a unique name for the profile and enter a description.

Step 4   Select **Carrier Ethernet** or **Optical** or **L3VPN** from the **Technology** list. The relevant service types for the selected technology are displayed.

Step 5   Select the required service type.

For L3VPN services, choose **Unicast** to create a profile that helps pre-populate values for most L3VPN service creation fields. And choose **IPSLA Operations** to create a profile with IP SLA specific options for the L3VPN service.

Step 6   Click **Next** to go to the attribute definition pages and define the attributes for the selected service type. The attributes in the profile are the same as the attributes in the Provisioning Wizard and they are described in the reference sections, as follows:

Information on Ethernet VCs attributes is provided in these topics:

- For attributes relating to the service itself, see Service Details Reference, on page 11
- For attributes specific to the UNI, see New UNI Details Reference, on page 12
- For attributes relating to the UNI as it operates within the service, see UNI Service Details Reference, on page 12.
- For QoS Profile attributes, see Create QoS Profiles, on page 78
- For UNI attributes, see Configure a Device and Interface To Be a UNI, on page 15
- For ENNI attributes, see Configure a Device and Interface To Be an ENNI, on page 16

Information on OCH and OTN attributes is provided in Circuit Section Reference for OCH Circuit Types, on page 19 and Circuit Section Reference for OTN Circuit Types, on page 30.

Information on L3VPN attributes is provided in Create and Provision a New L3VPN Service, on page 39 and View L3VPN Service Details, on page 48.

Step 7   Click **Create Profile** when you have defined the attributes. The profile will be added to the table in the Profiles window.

Create QoS Profiles

You can create a library of QoS profiles that will be available for selection when creating and provisioning EVCs. The selected QoS profile determines the bandwidth profile for traffic of various classes on the UNI or the EVC level, and defines how the classified traffic is treated.

The QoS profile can define up to four levels of bandwidth profile: Extra High, High, Medium, and Low. For each bandwidth profile, you specify the matching criteria that must be met for the traffic to be classified as belonging to that bandwidth profile.

To create a QoS profile:

Step 1   Follow the instructions in Create and Provision a New Carrier Ethernet EVC, on page 7 to access the Provisioning Wizard.

Step 2   Select **Carrier Ethernet** from the Technology drop-down list.

Step 3   Select **QoS Profile** from the Service Types drop-down list.

Step 4   Click **Next** to go to the QoS Profile definition page.

Step 5   Provide the QoS profile with a unique name and description.

Step 6   Check the required check boxes to define where the QoS profile will be available for selection (i.e., it will appear in the drop-down list of QoS profiles):

- Applicable for Interfaces—The QoS profile will be available for selection when provisioning UNIs or ENNIs.
- Applicable for Virtual Services—The QoS profile will be available for selection as a UNI service attribute when creating VLAN-based services, such as EVPL, EV-LAN, and so on.
- Applicable for Private Services—The QoS profile will only be available for selection as a UNI service attribute when creating private VCs, such as EPL, EP-LAN, and so on

Step 7   In the Classification field, indicate what method will be used to identify and classify the traffic, then enter the relevant values in the Match Criteria field for the required bandwidth profiles:

- DSCP—Differentiated service code point (DSCP) value will be used to classify the traffic. Valid values are from 0 to 63. Up to 8 comma-separated values can be entered.

- COS (Class of service)—Also known as PCP—IEEE 802.1Q bits in the header of the layer 2 frame from hosts supporting FCoe and other trunked devices.Valid values are from 0 to 7. Multiple comma-separated values or a range of values indicated by a hyphen (e.g., 0-2), can be entered.

Step 8   Select one or more classes of service that will apply to the service.

Step 9   For each class of service you selected, define a bandwidth profile to specify the match criteria and how the matching traffic will be handled.For each bandwidth profile, enter the match criteria, as described in Step 7 above.

Step 10   For each bandwidth profile, create rules to specify how the matching traffic will be handled. You can create a separate rule for ingress and egress traffic or you can create a rule for traffic moving in both directions. In each rule, you can specify the following:

- Committed Information Rate (CIR)—The long-term average transmission rate, specified in bits per second (bps).
- Committed Burst Size (CBS)—How large traffic bursts can be (in bytes) before some traffic exceeds the CIR.
- Excess Information Rate (EIR)—The average rate up to which packets are admitted. The EIR is greater than or equal to the CIR. Packets that exceed the CIR are typically discarded.
- Excess Burst Size (EBS)—How large traffic bursts can be (in bytes) before traffic exceeds the EIR.
- Color Mode—Specify whether traffic coloring will be applied or not.

Step 11   Click **Submit** when you have defined all the required bandwidth profiles. Your QoS profile will be created and will be available for selection when you are creating VCs.

Create Customers

Customers must be created in the system so that they are available for selection during the circuit/VC provisioning process.

To create a customer:

Step 1   From the left sidebar, choose **Inventory > Other > Customers**.

Step 2   Click **Create Customer**.

Step 3   Enter the name of the customer and a description (optional).

Step 4   Click **OK**. The customer is now added to the table of customers. You can select a customer to edit or delete it.

Provision a Circuit/VC with an Unmanaged Endpoint

You can create and provision a circuit/VC even if one or more of the endpoints is a device that is not managed by Cisco EPN Manager. The Provisioning Wizard allows you to identify an endpoint device as "unmanaged" and to provide information about that device so that the system can create the circuit/VC. Once you identify the unmanaged device, it will be available in the system in the Unmanaged Devices group and can be used for other services.

Step 1   Start the circuit/VC creation process for the required technology, as described in Provision Circuits/VCs, on page 1.

Step 2   For a point-to-point EVC and a CEM service:

   a) When defining the Z endpoint, select the **Unmanaged Device** check box. The Unmanaged Device Details panel opens.

   b) If the unmanaged device has already been identified in the system, deselect the **New Device** check box and select the required device from the list. If you are identifying a new unmanaged device, provide the device name, IP address, and LDP IP. The LDP IP is used as the neighbor address of the pseudowire on the managed device.

   c) Under Service Endpoint details, specify the virtual circuit identifier (VC ID). The VC ID field will be populated with the value of the VPN ID specified in the service details and will not be editable.

Step 3   For a point-to multipoint or multipoint -to-multipoint EVC: In the Unmanaged UNI page, click the Plus icon in the table to add a row and then define the Unmanaged Device Details and Service Endpoint details for the selected row.

Step 4   Complete the circuit/VC creation and provisioning process for the required technology, as described in Provision Circuits/VCs, on page 1.

Extend a Circuit/VC Using Templates

When you create and provision a circuit/VC, Cisco EPN Manager configures a set of CLI commands on the participating devices. If you need to configure additional commands on the same devices, you can create a template containing these commands and you can include it during the circuit/VC creation process. This effectively extends the circuit/VC beyond what is configured by Cisco EPN Manager. This functionality is available in the provisioning wizard but it is dependent on the template being created prior to creating or modifying the circuit/VC.

Extending a circuit/VC using CLI templates involves the following steps:

1. Create the CLI template using blank templates or existing templates. See Create a New CLI Configuration Template Using a Blank Template and Create a New CLI Configuration Template Using An Existing Template.

2. Create/modify a circuit/VC and append the CLI template. See Provision Circuits/VCs, on page 1.

Step 1   Create the CLI template:

   a) In the left sidebar, choose **Configuration > Templates > Features & Technologies**.

b) In the Templates panel, choose **CLI Templates > CLI**.

c) Provide identifying information for the new circuit and define the content of the template using CLI, global variables, and/or template variables. See Creating CLI Templates and Use Global Variables in a Template.

d) Click **Save as New Template**.

e) The new CLI template is saved under **My Templates > CLI Templates (User Defined)**.

Step 2   Create/modify a service that includes the template you created (or a different template if relevant):

a) From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

b) Click the **Circuits/VCs** tab.

c) From the **Circuits/VCs** pane toolbar, either click the + (**Create**) icon or select a circuit and then click the pencil (**Modify**) icon.

The Provisioning Wizard opens in a new pane to the right of the map.

d) Start creating or modifying the required circuit or VC. See Provision Circuits/VCs, on page 1 and Modify a Circuit/VC.

e) In the **Service Template** page, use the **Pre-Configuration** section if you want the template to be a prefix to the service configuration or use the **Post-Configuration** section if you want the template to be a suffix to the service configuration.

f) In the **Template** drop-down menu, select the required CLI template.

The same CLI template cannot be selected for both pre-configuration and post-configuration options.

g) In the **Template Usage** drop-down menu, select an option to indicate under what circumstances the CLI template should be configured on the devices. For example, if you select **Service Create Only**, the template CLI will only be configured on the devices when the service is created. It will not be configured when the service is modified.

h) Enter values for the template parameters. The parameters shown here depend on the variables that were defined for the template.

i) Click **Submit**.

Note   By default, the selected CLI templates are associated with all devices that take part in the service. You cannot specifically choose the devices to be associated with the CLI templates.

Example Configuration: Extend a Circuit/VC Using CLI Templates

Example Configuration 1: Extending an L3VPN service on a Cisco ASR 903 device using a CLI template with Global and Template (Local) variables:

```
vrf definition Testdoc1
exit
vrf Testdoc1
  vpn id 36B:3
  address-family ipv4 unicast
    import route-target
      65:1
    export route-target
      65:1
  address-family ipv6 unicast
    import route-target
      65:1
```

```
      export route-target
        65:1
interface  GigabitEthernet0/0/0/11.2
  vrf   Testdoc1
  ipv4 address 4.5.7.8 255.255.255.0
  mtu 1522
router bgp 140
  vrf  Testdoc1
    rd auto
    address-family ipv6 unicast
    address-family ipv4 unicast
      redistribute static metric 54
    neighbor 3.4.6.8
      remote-as 21
      address-family ipv4 unicast
        exit
      exit
    exit
  exit
  interface GigabitEthernet0/0/6
  desc postconfig
  delay 5988
  mtu 436
  exit
```

Example Configuration 2: Extending a CEM service using a CLI template with a global variable and a template (local) variable:

```
#set($interfaceNameList = $gv.service-cem-cemInterfaceNameList.split(","))
#set($cemGroupNumberList = $gv.service-cem-cemGroupNumberList.split(","))
#set($count = 0)
#foreach($interfaceName in $interfaceNameList)
  interface $interfaceName
    service-policy input MainInterfacePolicy
    #if($count == 0)
      cem $cemGroupNumberList[0]
    #else
      cem $cemGroupNumberList[1]
    #end
        service-policy input servicePolicy
    #set($count = $count+1)
#end
```

Example Configuration 3: Extending a CEM service to configure QoS over CEM:

```
#set($count = 0)
#foreach($interfaceName in $gv.service-cem-cemInterfaceNameList)
interface $interfaceName
service-policy input MainInterfacePolicy
#if($count == 0)
cem $gv.service-cem-cemGroupNumberList[0]
#else
cem $gv.service-cem-cemGroupNumberList[1]
#end
service-policy input servicePolicy
#set($count = $count+1)
#end
exit
```

Example Configuration 4: Extending a CE service using a CLI template with global and template variables on a Cisco ME3800 device. The highlighted text represents the pre-config and post-config configuration changes that are appended and prepended to the CE service provisioning configuration.

```
pseudowire-class PWClass_51_192-168-12-29
protocol ldp
exit
ethernet cfm domain EVC level 4
  service evplextnpseudowireclass_ evc evplextnpseudowireclass_
    continuity-check
    continuity-check interval 1s
ethernet evc evplextnpseudowireclass
interface GigabitEthernet0/11
  no shutdown
  no spanning-tree portfast
  mtu 1522
  ethernet uni id 3800x
  service instance 1 ethernet evplextnpseudowireclass
    encapsulation dot1q 88
    xconnect 192.168.12.29 51 encapsulation mpls  pw-class PWClass_51_192-168-12-29
      mtu 1508
  service instance 1 ethernet evplextnpseudowireclass_
    cfm mep domain EVC mpid 2
    ethernet lmi ce-vlan map 88
ip sla 17
  ethernet y1731 loss SLM domain EVC evc evplextnpseudowireclass_ mpid 1 cos 5 source mpid
 2
    history interval 5
    aggregate interval 60
ip sla schedule 17 life forever start-time after 00:02:00
interface GigabitEthernet0/11
desc postconfig
exit
```

Example Configuration 5: Extending a Layer 3 Link service using a CLI template with a global variable and a template (local) variable:

```
##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
 ##XE DEVICE
 #if($variant=="IOS-XE")
 #if($gv.service-l3Link-routingProtocolName=="BGP")
   router bgp $gv.service-l3Link-routerProcessId
           address-family ipv4
          neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
    ##assume A End as remote building
          #if($gv.service-l3Link-isRouteReflectorClient=="TRUE" && $prefixListName!="" &&
 $gv.service-l3Link-endPointDesignation=="AEND")
    neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list send
              neighbor $gv.service-l3Link-bgpNeighborName prefix-list $prefixListName
in
              #elseif($gv.service-l3Link-isRouteReflectorClient=="TRUE" &&
$prefixListName!="" && $gv.service-l3Link-endPointDesignation=="ZEND")
    neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list receive
          #end
              exit
        exit
      #end

      #if($xeMTU!="" || $xeClnsMTU!="")
       interface $gv.service-l3Link-interfaceName
        #if($xeMTU!="")
            mtu $xeMTU
        #end
        #if($xeClnsMTU!="")
            clns mtu $xeClnsMTU
        #end
```

```
                                  exit
                       #end

                       #if($gv.service-l3Link-routingProtocolName=="BGP")
                       #if($addressFamily !="" && $addressFamily=="vpnv4")
                        router bgp $gv.service-l3Link-routerProcessId
                          address-family $addressFamily
                           neighbor $gv.service-l3Link-bgpNeighborName activate
                   neighbor $gv.service-l3Link-bgpNeighborName send-community both
                   #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
                   neighbor $gv.service-l3Link-bgpNeighborName route-reflector-client
                   #end
                   bgp additional-paths install
                   neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
                           exit
                       exit
            #end
            #end
            ##XR DEVICE
            #else

             #if($xrMTU!="")
             #if($gv.service-l3Link-subInterfaceName!="")
                          interface $gv.service-l3Link-subInterfaceName
                               mtu $xrMTU
                           exit
                      #else
                          interface $gv.service-l3Link-interfaceName
                               mtu $xrMTU
                           exit
                       #end
                   #end

                   #if($gv.service-l3Link-routingProtocolName=="BGP")
                   #if($addressFamily !="" && $addressFamily=="vpnv4")
                    router bgp $gv.service-l3Link-routerProcessId
                      address-family $addressFamily unicast
                 additional-paths receive
                          exit
                      neighbor $gv.service-l3Link-bgpNeighborName
                       address-family $addressFamily unicast
                                #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
                       route-reflector-client
                                #end
                      aigp
                                #if( $routePolicyName!="")
                       route-policy $routePolicyName in
                                #end
                             exit
                           exit
                       exit
                   #end
                   #end


             #end

            ##DELETE USE CASE
            #elseif($gv.service-serviceOperationType == "DELETE")
             ##XE DEVICE
             #if($variant=="IOS-XE")

                   #if($xeMTU!="" || $xeClnsMTU!="")
                    interface $gv.service-l3Link-interfaceName
```

```
                #if($xeMTU!="")
                        no mtu $xeMTU
                #end
                #if($xeClnsMTU!="")
                        no clns mtu $xeClnsMTU
                #end
                    exit
            #end

             #if($gv.service-l3Link-routingProtocolName=="BGP")
             #if($addressFamily !="" && $addressFamily=="vpnv4")
              router bgp $gv.service-l3Link-routerProcessId
               no address-family $addressFamily
                 exit
            #end
            #end


  ##XR DEVICE
  #else
   #if($xrMTU!="")
     #if($gv.service-l3Link-subInterfaceName=="")
                 interface $gv.service-l3Link-interfaceName
                     no mtu $xrMTU
                  exit
            #end
        #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily !="" && $addressFamily=="vpnv4")
         router bgp $gv.service-l3Link-routerProcessId
          address-family $addressFamily unicast
     no additional-paths receive
     exit
     neighbor $gv.service-l3Link-bgpNeighborName
           no address-family $addressFamily unicast
     exit
             exit

        #end
        #end

 #end

#end
```

Example Configuration 6: Extending a Bidirectional TE tunnel using a CLI template with a global variable and a template (local) variable:

```
##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
  #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
         #if($xeBandWidth && $xeBandWidth !="")
                interface Tunnel$gv.service-teTunnel-tunnelId
                   bandwidth $xeMaxBandWidth
                      tunnel mpls traffic-eng auto-bw frequency $xeBandWidth max-bw
$xeMaxBandWidth min-bw $xeMinBandWidth
                exit
          #end
    #end
 #else
      #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
     #if($xrBandWidth && $xrBandWidth!="")
```

```
                    interface tunnel-te$gv.service-teTunnel-tunnelId
                        bandwidth $xrMaxBandWidth
                        auto-bw
                            bw-limit min $xrMinBandWidth max $xrMaxBandWidth
                        application $xrBandWidth
                    exit
                exit
            #end
    #end
    #end
#elseif($gv.service-serviceOperationType == "DELETE")
 #if($variant && $variant=="IOS-XE")
            #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
     #if($xeBandWidth && $xeBandWidth!="")
                    interface Tunnel$gv.service-teTunnel-tunnelId
                        no bandwidth
                        no tunnel mpls traffic-eng auto-bw
                    exit
            #end
      #end
 #else
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
            #if($xrBandWidth && $xrBandWidth!="")
                    interface tunnel-te$gv.service-teTunnel-tunnelId
                        no bandwidth
                        no auto-bw
                    exit
            #end
    #end
    #end

#end
```